Digital Cooperation Organization

The Hellenic Republic

Greece

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, 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.

Cross-Border Data Transfers

Data flows to the European Union (EU) 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

Location of Computing Facilities:

Neither national law in Greece nor EU law mandates data localisation in general. A localisation requirement applies to electronic communications services in Greece. A similar requirement was invalidated at the EU level.

Online Consumer Protection:

Greece protects online consumers via its general consumer protection framework, which prohibits making misrepresentations and charging consumers without authorisation. The sending of unsolicited messages (spam) is prohibited as an "aggressive commercial practice" but is allowed if the subscriber expresses prior consent.

Electronic Transactions:

Greece's electronic transactions framework comprises several binding legal acts at the national and EU level. Electronic transactions are recognised as equivalent to paper-based transactions. The framework distinguishes between electronic signatures, advanced electronic signatures, and qualified electronic signatures, which are recognised as equivalent to hand-written signatures.

Trade Facilitation with Digital Means:

Greece provides trade administration documents in electronic form and enables electronic submission for such documents. Greece has established the National Single Window as the electronic one-stop service to facilitate trade within and outside the EU.

Cybersecurity:

Cybersecurity obligations are tiered. Essential and important entities must uphold enhanced security requirements and notify cybersecurity incidents to authorities and users. Personal data breaches must generally be notified to authorities and data subjects.

Artificial Intelligence:

Greece's AI regulatory framework comprises the national law on emerging technologies and digital governance, as well as the EU AI Act. The AI Act establishes obligations based on AI risk categories, mainly focusing on "high-risk AI systems", and technology-specific rules for general purpose AI models.

Source Code:

Greece protects computer programmes as works of authorship, granting economic and moral rights with certain exceptions. Greece can demand source code sharing in the context of software development for public sector bodies. The EU AI Act further demands government access to source code 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.

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. Greece does not impose specific direct taxes on providers of digital services and products.

Electronic Payments:

Greece applies both general payment rules and specific rules on electronic payments. Know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to electronic payment providers.

SMEs and Digital Inclusion:

Greece has implemented a range of initiatives to support SMEs and disadvantaged groups in leveraging digital technologies for trade. These measures include national strategies, funding programmes, and participation in EU-wide digital transformation efforts.

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.

Greece 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 Hellenic Data Protection Authority is in charge of oversight and regularly publishes enforcement action, including 12 fines, as well as several reprimands and warnings since 2023.

Summary

- The Greek data protection law implements the EU's General Data Protection Regulation (GDPR). It ensures the protection of personal data, setting requirements for lawful processing, and data security. Data subjects 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 on the protection of personal data and privacy in the electronic communications sector, in effect since 2006, introduces strict enforcement mechanisms for data protection violations. The law on emerging information and communication technologies and strengthening digital governance, enacted in 2022 and later amended in 2024, regulates the processing of personal data when using artificial intelligence systems. Greece 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 Hellenic Data Protection Authority (HDPA) is an independent public authority responsible for supervising the processing of personal data. The HDPA issues guidelines, handles complaints, carries out investigations, and establishes certification mechanisms.

- The Hellenic Data Protection Authority has issued several "regulatory acts" related to data protection, including on the data protection assessment, informing data subjects of personal data processing through the press, and conditions for the lawful processing of personal data for the purposes of direct marketing or advertising and credit rating. In addition, since 2023, the authority has issued 12 fines, as well as reprimands and warnings.

- Finally, the Digital Transformation Bible 2020-2025, aims to integrate data protection into Greece's digital transformation. It includes the development of an integrated information system, which will provide data subjects as well as data controllers and processors with appropriate electronic services.

SOURCES

Primary Legislation

- Law 4624/2019 | Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679...and transposition of Directive (EU) 2016/680...
- Law 3471/2006 | Protection of personal data and privacy in the electronic telecommunications sector (Law Amendment 2472/1997)
- Law 4961/2022 | Emerging information and communication technologies, strengthening digital governance (Law Amendment 3783/2009)
- 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...

Secondary Legislation

- - Regulatory Act B' 3433/31.12.2013

Guidelines

- Digital Transformation Bible 2020-2025
- Hellenic Data Protection Authority: Regulatory Act 408/1998
- Hellenic Data Protection Authority: Regulatory Act 26/2004
- Hellenic Data Protection Authority: Regulatory Acts of the DPA
- Hellenic Data Protection Authority: Data Protection Impact Assessment
- Hellenic Data Protection Authority: Guidelines for Individuals
- Hellenic Data Protection Authority: Guidelines for Organisations
- EU Working Party: Working Document 02/2013 providing guidance on obtaining consent for cookies
- EU Working Party: Opinion 04/2012 on Cookie Consent Exemption

Oversight Authorities

- Hellenic Data Protection Authority - HDPA

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.

Summary

- In Greece, cross-border data transfers are regulated under the General Data Protection Regulation (GDPR), applicable across the EU. The Greek Data Protection Law of 2019 mandates the Hellenic Data Protection Authority (HDPA) 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.

- 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 Greece. The country aligns with the EU's guidelines.

SOURCES

Primary Legislation

- Law 4624/2019 | Hellenic Data Protection Authority (HDPA)
- 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.

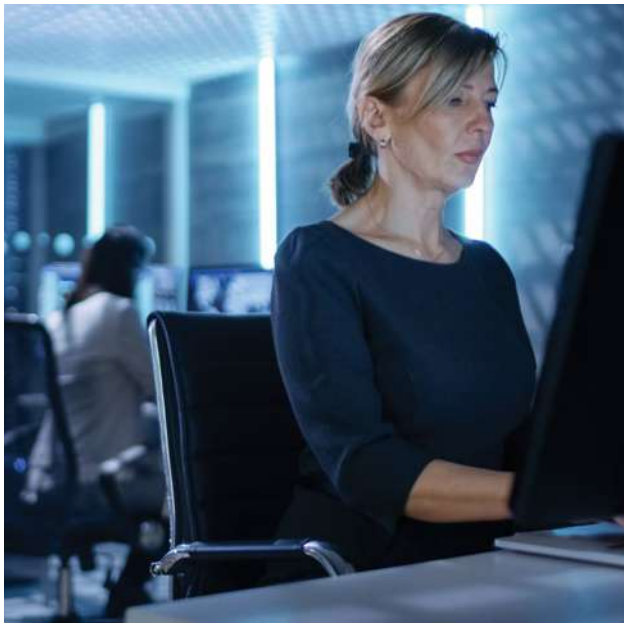
Neither national law in Greece nor EU law mandates data localisation in general. A localisation requirement applies to electronic communications services in Greece. A similar requirement was invalidated at the EU level.

Summary

- Neither the EU General Data Protection Regulation nor the Greek data protection laws mandate general data localisation, although conditions for cross-border transfers apply (see the section on Cross-Border Data Transfer above). However, electronic communications services in Greece must localise data.

- Specifically, the 2011 law on the retention of data from electronic communications services requires that data is stored on physical media located within the Greek territory. After the 12 month retention period, the data must then be destroyed by the provider, with exceptions for data that has been lawfully accessed.

- The EU Data Retention Directive, which included a similar requirement, was invalidated by the Court of Justice of the European Union in a 2014 ruling.



SOURCES

Sources

- Law 3917/2011 | Retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks, the use of surveillance systems for the reception or recording of sound or images in public places and related provisions
- 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

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.

Greece regulates online consumer protection via its general consumer protection framework, especially the consumer protection law. Prohibited practices include making misrepresentations, failing to deliver products or services after charging consumers, and charging consumers without authorisation.
E-commerce platforms are not subjected to indirect obligations but are subject to requirements regarding transparency and non-discrimination (in ranking lists). Spam is prohibited as an "aggressive commercial practice" but is allowed if the subscriber expresses prior consent. The Directorate-General for Market and Consumer Protection under the Ministry of Development is in charge of oversight and publishes enforcement information, including two fines since 2023.

Summary

- The Consumer Protection Law establishes fundamental rights for consumers, including protection against unfair commercial practices and unsafe products. It mandates clear and accurate information about products and services. The law provides mechanisms for consumers to seek redress and compensation if their rights are violated. The 2018 consolidated version of the Consumer Protection Law prohibits practices including false information and charging consumers without permission. In addition, the law on strengthening the consumer protection framework 2023, enhances the enforcement mechanisms in the digital space, establishing procedures for consumers to file complaints and conditions under which consumers can withdraw from digital content. Finally, the law on the protection of personal data and privacy in the electronic communications sector prohibits unsolicited communication unless the subscriber gives its prior consent.

- As a member of the EU, Greece incorporates several EU consumer protection rules. Recently, the Greek law on the modernisation of EU rules on consumer protection law transposed several EU directives on consumers in the digital age. Specifically, it transposed the EU directives on consumer rights in the digital space, online dispute resolution, and better enforcement and modernisation of the EU's consumer protection rules. It also transposed rules concerning cooperation between online platforms and national authorities to enforce consumer protection.

- In addition, the Digital Content and Services Law 2022 incorporated certain provisions of the EU Digital Services Act. The Digital Services Act establishes 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 Directorate-General for Market and Consumer Protection, under the Ministry of Development, oversees consumer protection. It handles consumer complaints and enforces consumer protection rules, including 2 fines in 2023. In addition, the National Consumer and Market Council proposes measures to enhance consumer rights, provides opinions on related legislation, and advises on the protection of consumer interests.

- Several Ministerial Decisions touch upon consumer protection, for example regarding enforcement, non-discrimination, and online dispute resolution. In addition, Greece has adopted a Consumer Code of Conduct and a regulation approving the rules of procedure of the National Council of Consumer and Marketing (NCCM). Currently, Greece is deliberating a Practical Guide for the Protection of Consumers in price reduction announcements.

SOURCES

Primary Legislation

- Ministerial Decision No. 5338/17.1.2018 | consolidated consumer protection law
- Law 3471/2006 | Protection of personal data and privacy in the electronic communications sector and amendment of Law No. 2472/1997
- Law 5019/2023 | ...Strengthening consumer protection...
- Law 4933/2022 | Modernisation of EU Rules on consumer protection
- 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

- Regulation 1596/2016 | Approval of the Rules of Procedure of the National Consumer and Market Council (NCCM)
- Ministerial Decision 14486/15.2.2023 | enforcement on consumer protection
- Ministerial Decision 22998/20.3.2024 | non-discrimination & online dispute resolution
- Ministerial Decision 18898/13.2.2019 | Non-discrimination & Consumer Protection
- Presidential Decree 10/2017 | Consumer Code of Conduct

Guidelines

- Ministry of Development: Practical Guide for the protection of consumers in all price reduction announcements

Oversight Authorities

- Directorate-General for the Market and Consumer Protection (Consumer Protection Sector) - DGAPK
- National Consumer and Market Council - ESKA

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.

Greece's electronic transactions framework comprises several binding legal acts at the national and EU level. Electronic transactions are recognised as equivalent to paper-based transactions. The framework distinguishes between electronic signatures, advanced electronic signatures, and qualified electronic signatures, which are recognised as equivalent to hand-written signatures. Greece 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

- The Greek digital governance and electronic law of 2020 recognises electronic transactions as equivalent to paper-based transactions. Electronic documents hold the same legal status and value as paper documents, when signed with an electronic signature that meets specific criteria. The Law differentiates electronic signatures from advanced electronic signatures and qualified/approved electronic signatures, the latter carrying the same legal weight as handwritten signatures. 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. Finally, the governmental authentication service in Greece secures digital identity verification and authentication for public sector services. The emerging communication technologies law of 2022 regulates the legal validity, proof of registration, and the execution of smart contracts using approved electronic signatures or seals.

- The Trust Services Department of the e-Government Directorate of the Ministry of Digital Governance provides personal digital authentication/signature certificates free of charge. The Hellenic Telecommunications and Post Commission supervises electronic communications and oversees the use of electronic signatures and trust services to ensure compliance related to electronic transactions and signatures.

- The Greek 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.

- Finally, Greece 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.

SOURCES

Primary Legislation

- Law 4727/2020| Digital Governance & electronic communications
- Law 4961/2022 | Emerging Communication Technologies
- Law 4601/2019 | Harmonisation with EU Directive on e-invoicing
- Law 3979/2011 | Use of Information & Communication Technologies (e-government law)
- Law 4070 (82/A/2012) | Electronic Communications, Transport, Public Works and other provisions
- 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

Secondary Legislation

- Regulation No 248/71 of the Hellenic Telecommunications and Post Commission - EETT | Regulation for the Provision of Electronic Signature Certification Services
- D. 1034/2020 | Obligations of Electronic Data Issuance Service Providers and control procedures for the provision of electronic data issuance services
- Presidential Decree 2403/2024 | Certification Regulation of the Hellenic Public Sector Certification Authority
- 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
- 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

- Greek Public Sector Certification Authority (e-signatures)
- The Hellenic Telecommunications and Post Commission (EETT) | for e-signatures

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.

Greece provides trade administration documents in electronic form and enables electronic submission for such documents. Greece has established the National Single Window as the electronic one-stop service to facilitate trade within and outside the EU. 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

- The Greek law on improving the business environment of 2012 established the electronic trade single window. It mandates that through the window, businesses shall electronically submit applications and documents for certificates and authorizations as required by law, and these documents are processed electronically by the relevant authorities. The National Single Window (also referred to as the National Maritime Single Window) is integrated into broader systems to enhance trade efficiency both within the EU and with third countries. In addition, the Greek Customs System ICISnet enables users to electronically submit declarations. The ICISnet Import Subsystem manages the process of importing goods from non-EU countries, whether for free circulation or under special import schemes. The Independent Authority for Public Revenue (IAPR) certifies and collects tax, customs and other public revenues. The authority has issued several instructions and circulars on the procedure for the electronic submission of the customs declaration and its supporting documents.

- The Greek 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, Greece 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. The Independent Authority for Public Revenue has published instructions on the customs import procedures.

- 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.

- In addition, the Digital Transformation Bible 2020-2025 includes an action plan on the implementation of the Single Window system. Additionally, the trade facilitation roadmap 2022-2026 focuses on simplifying, harmonising, and digitising trade procedures to improve Greece's role in international trade. Greece also adheres to the European guidelines. The electronic customs multi-annual strategic plan of 2023 focuses on aligning with the Union Customs Code (UCC) and ensuring the effective management of electronic customs projects.

SOURCES

Primary Legislation

- Law 4072/2012 | Improving the business environment
- Law 4529/2018 | Incorporation into Greek legislation of Directive 2014/104/EU of the European Parliament and other provisions
- 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

- Independent Authority for Public Revenue: Directive: Customs import procedures and procedures for the refund of value added tax on the import of goods of small value (up to the amount of EUR 150) subject to distance selling (e-commerce) from 1/7/2021" - Intra-Community distance sales of products subject to excise and excise duties
- Independent Authority for Public Revenue: Imports System: Customs Procedures and e-services directives
- Independent Authority for Public Revenue: Instructions on the procedure for the electronic submission of the customs declaration and other customs documents within the framework of the ICISnet Import subsystem (2013)
- Independent Authority for Public Revenue: Circular: Compulsory electronic submission of supporting documents of the import declaration - Record-keeping (2016)
- Trade Facilitation RoadMap 2022-2026
- Digital Transformation Bible 2020-2025
- EU: Electronic Customs Multi-Annual Strategic Plan for Customs 2023
- European Commission: Customs formalities for low value consignments (duty de minimis threshold)
- European Commission: Buying goods online coming from a non-European Union country
- European Commission: VAT One Stop Shop
- National Maritime Single Window
- Independent Authority for Public Revenue: E-Transactions

Oversight Authorities

- Independent Authority for Public Revenue - IAPR

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.

Greece's regulatory framework for cybersecurity comprises several legal acts at the national and EU level. Cybersecurity obligations are tiered, for example demanding enhanced security from essential and important entities. Such entities must further notify cybersecurity incidents to government authorities and users. In addition, personal data breaches must be notified to authorities and data subjects. Oversight is divided between the National Intelligence Service, the General Directorate of Cybersecurity, the Computer Security Incident Response Team, the Directorate of Cyber Defense, and sectoral bodies. Currently, a National Cybersecurity Authority is being established. There is currently no public, central repository of enforcement action regarding cybersecurity.

Summary

The Law on cybersecurity and protection of citizens' personal data 2022 was enacted to strengthen Greece's cybersecurity framework. It imposes security obligations on operators, defines penalties, aligns with European standards, and addresses emerging cyber threats. The law on emerging information and communication technologies, enacted in 2022, establishes guidelines for the protection of critical infrastructure and key digital services. It mandates comprehensive cybersecurity measures for both public and private sector entities. It also defines the responsibilities of the National Cybersecurity Authority and the Internet Security Officers. In February 2024, the law on the establishment of the National Cybersecurity Authority came into force. The Authority will be monitoring and controlling compliance with the legal framework for cybersecurity, imposing sanctions and developing a certification framework for cybersecurity products and services. Finally, the Greek National Intelligence Service (NIS) Law, which was amended in 2024, mandates protection measures and responsibilities, including risk assessment and security audit.

Greece, as a member of the EU, incorporated several cybersecurity rules in its legal framework.

01 It complies with the Regulation establishing the European Cybersecurity, Industrial, Technology and Research Competence Centre 2021.

02 It 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 Greek legislation by 2024.

Under article 23 of the NIS 2 Directive, essential and important entities are required 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 a Regulation.

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

06 Finally, the EU GDPR requires personal data breaches to be notified to authorities and data subjects.

The General Directorate of Cybersecurity, established in 2018 under the Ministry of Digital Governance, formulates and coordinates cybersecurity policies and oversees the implementation of the National Cyber Security Strategy.

It coordinates with other relevant authorities:

01 The Hellenic Computer Security Incident Response Team (CSIRT) is Greece's cyber defence, incident response, and operational integration centre.

02 The Directorate of Cyber Defence of the Hellenic National Defence General Staff focuses on the protection and defence of the national defence's information and communication systems.

03 The National Intelligence Service (NIS) is the government agency responsible for safeguarding national security and expanded its focus to prioritise cybersecurity in 2020. Its objectives are to prevent, avert, deter and neutralise espionage and terrorist threats.

04 The Cyber Crime Division is an independent central service of the Hellenic Police whose mission includes the prevention, investigation, and repression of crimes committed through the Internet or other means of electronic communications.

05 The Hellenic Authority for Communication Security and Privacy (ADAE) is a constitutionally consolidated independent authority, responsible for securing electronic communications and privacy. Together with the National Data Protection Authority (HDPA) they receive data breach notifications.

The consumer protection framework is complemented by secondary legislation and guidance:

01 The Ministerial Decision of 2019 focuses on enhancing cybersecurity in Greece and sets out the details for implementing the provisions of the law that adopts the EU's Network and Information Systems Directive. It establishes measures for protecting networks, information systems and digital service providers.

02 Greece's National Cybersecurity Strategy 2020-2025 aims to enhance the country's digital security infrastructure. The strategy emphasises public-private partnerships to foster innovation in cybersecurity technologies. It also prioritises boosting Greece's capabilities in mitigating cyber threats.

03 The Digital Transformation Bible 2020-2025 includes projects for enhancing cybersecurity. These actions feature the development of national risk assessments and contingency plans for cyber crises. They also include the establishment of a platform for sharing information related to cybersecurity threats and a real-time monitoring system.

04 The Cybersecurity Handbook 2021 includes practical guidelines, best practices, and resources for identifying, preventing, and responding to cyber threats, emphasising the importance of a proactive approach to cybersecurity.

05 There is currently no centralised database for enforcement action on cybersecurity. Several complaint cases related to new-technologies were handled based on the Hellenic Data Protection Authority 2022 report.

SOURCES

Primary Legislation

Greece

- Law 5086/2024 | National Cyber Security Authority and other provisions
- Law 5002/2022 | Procedure for lifting the confidentiality of communications, cybersecurity and protection of citizens' personal data
- Law 4961/2022 | Emerging Communication & Information Technologies
- Law 3649/2008 | National Intelligence Service
- 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)
- Secondary Legislation
- Ministerial Decision 1027/2019 | on Law 4577/2018
- Presidential Decree 40/2020 (consolidated)

Guidelines

- National Cybersecurity Authority: National Cybersecurity Strategy 2020-2025
- National Cybersecurity Authority: Cybersecurity Handbook 2021
- HDPA: Annual Report 2022
- Digital Transformation Bible 2020-2025

Oversight Authorities

- National Intelligence Service - NIS
- General Directorate of Cybersecurity
- Hellenic Computer Security Incident Response Team - CSIRT
- Directorate of Cyber Defense | Hellenic National Defense General Staff
- Cyber Crime Division | Hellenic Police
- Hellenic Data Protection Authority - HDPA
- Hellenic Authority for Communication Security and Privacy - ADAE
- European Union Agency for Cybersecurity - ENISA

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.

Greece's AI regulatory framework comprises the national law on emerging technologies and digital governance, as well as the EU AI Act. 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. The law on emerging technologies and digital governance, however, explains how privacy rules apply to AI training.

Summary

- The Greek law on emerging information and communication technologies (2022), introduces a national framework to regulate the use of AI technologies in the public and private sectors. The law establishes a Coordinating Committee for AI with responsibilities for drafting and formulating AI strategies and policies. It also sets up a committee for the supervision of the strategy and outlines how privacy regulations apply to AI training.

- Greece, as a member of the EU, 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.

- Greece does not currently have a dedicated AI authority yet. The Hellenic Ministry of Digital Governance is responsible for coordinating digital transformation efforts, including initiatives related to AI. Sectoral agencies cover AI in their respective domains.

- The Digital Transformation Bible 2020-2025, includes projects for developing AI. These actions determine the ethical principles for the AI use, describe national priorities and areas for maximising the benefits of AI and propose interventions.

- Generative AI Greece 2030 is the empirical strategic research approach and presents trends, opportunities, challenges, uncertainties and options that may shape the future of the AI ecosystem in the country. It further provides a framework of proposed strategic initiatives and policy recommendations.

SOURCES

Sources

Primary Legislation

- Law 4961/2022 | Emerging information and communication technologies, strengthening digital governance and other provisions
- Regulation (EU) 2024/1689 | 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

- Digital Transformation Bible 2020-2025
- Generative AI Greece 2030

Oversight Authorities

- The Hellenic Ministry of Digital Governance

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.

Greece's Intellectual Property law protects computer programmes as works of authorship. The protection extends to economic and moral rights, among others, although exceptions apply, for example modifications and backups by authorised users. Greece mandates source code sharing in the context of software development for public sector bodies, who can be granted access to the source code to understand, adapt and redistribute the code. 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 protects computer programmes and their design materials as works of authorship, if they are original creations. The protection extends to economic and moral rights, although exceptions are foreseen. Specifically, legally authorised users of the software can modify, back up, and study computer programs without the author's permission if necessary for their intended use. The Hellenic Copyright Organisation protects the authors and rights holders.

- The e-government law states that public sector bodies should be allowed to access, modify, and redistribute source code when procuring software development. The law specifies that the distribution, publication or availability of software products may be restricted if such actions violate state or legal confidentiality protections.

- In addition, 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 3979/2011| e-government law
- Law 2121/1993 | Intellectual property, related rights and cultural issues
- Regulation (EU) 2024/1689 of the European Parliament and of the Council | EU Artificial Intelligence Act
- Directive 2009/24/EC | on the legal protection of computer programs

Secondary Legislation

- Presidential Decree 311/1994 | Statute of the Intellectual Property Organisation
- Guidelines
- Open Source Software Strategy 2020–2023 by the EU
- Open Source Software Country Intelligence Report Greece 2020 | European Commission

Oversight Authorities

- Hellenic Copyright Organisation | Ministry of Culture

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.

Greece does not apply customs duties to digital services or products but applies value-added tax (VAT) thereto. Regarding e-commerce imports, Greece applies customs duties as well as VAT. Greece 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. Greece 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, Greece 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 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, Greece 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, a 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 Independent Authority for Public Revenue oversees the collection of taxes and customs duties, and the operation of the ICISnet platform for electronic submission and payment of taxes and duties. The Authority has published instructions on VAT and its application in e-commerce, OSS and customs import procedures on goods of small value. The European Commission has also issued several explanatory notes and guidelines on its VAT e-commerce rules.

SOURCES

Primary Legislation

- Law 2859/2000 | Ratification of the Value Added Tax Code
- Law 4818/2021 | a) Incorporation into Greek legislation of the provisions of Directives (EU) 2017/2455, (EU) 2019/1995 and (EU) 2018/1910 concerning obligations arising from value added tax on supplies of services and distance sales of goods and related provisions
- 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

Guidelines

- IAPR: Notice of Regulation EU with No. 952/2013 on the establishment of the Union Custom Code (UCC)
- IAPR: Notice of the Union Custom Code (UCC) legislative package
- Manual of instructions and case study in the context of the application of VAT to e-commerce | IAPR
- Circular: Customs import procedures and procedures for the refund of value added tax on the import of goods of small value (up to the amount of EUR 150) subject to distance selling (e-commerce) from 1/7/2021 - Intra-Community distance sales of products subject to excise and excise duties
- VAT on Imports - Exports / General Information -

July 2024 | IAPR
- E-commerce and VAT Special Schemes OSS/IOSS Explanatory Note | IAPR
- 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
- European Commission: Remarks by Commissioner Gentiloni at the Eurogroup press conference
- Buying goods online coming from a non-European Union country
- VAT e-commerce | gov.gr official website
- European Commission: VAT One Stop Shop
- European Commission: The One Stop Shop
- European Commission: What is the Common Customs Tariff?
- European Commission: Harmonised System
- EU: Taric
- European Commission: Explanatory Notes on VAT e-commerce rules
- IAPR: AEO - Authorised Economic Operators

Oversight Authorities

- Independent Authority for Public Revenue - IAPR

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

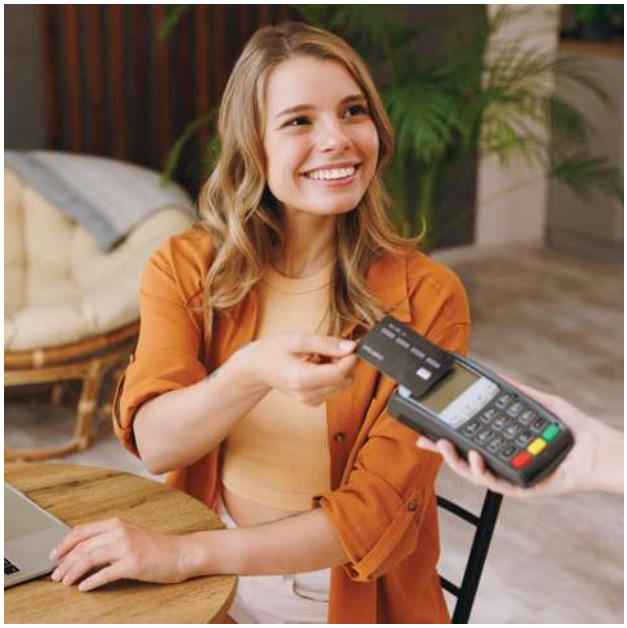
We outline whether there is a regulatory framework specifically addressing electronic payments. We then distil know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to electronic payments. In addition, we delineate licensing requirements and procedures for entities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

Greece 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. Greece has transposed these EU rules and demands an operating licence from the Bank of Greece to provide payment services.

Summary

- Greece's electronic payments framework is based on two EU directives that were transposed into national law. The EU directive on payment services (PSD2), establishes the regulatory framework for electronic payments across the EU. It specifies know-your customer (KYC), anti-money laundering (AML), and counter-terrorism-financing (CTF) rules that apply to electronic payments. 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.

- These obligations were transposed into the Greek regulatory framework. In addition, the Greek law on the prevention and suppression of money laundering and terrorist financing includes provisions for electronic money institutions. The Bank of Greece is responsible for overseeing electronic payments and has published several acts and guidelines. Payment institutions must obtain an operating licence from the Bank of Greece.



SOURCES

Primary Legislation

- Law 4537/2018 | Implementation in Greek legislation of Directive 2015/2366/EU on payment services and other provisions
- Law 5019/2023 | Implementation of the Directive (EU) 2020/1828...strengthening consumer protection...
- Law 4141/2013 | development investment instruments, provision of credit and other provisions
- Law 4557/2018 | Prevention and suppression of money laundering and terrorist financing (incorporation of Directive 2015/849/EU) and other provisions
- 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)

Secondary Legislation

- Bank of Greece Executive Committee Act 158/5/10.05.2019 | Adoption of guidelines by the European Banking Authority on conditions for granting an exemption from the emergency mechanism Article 33.6 of Regulation (EU)2018/389
- Bank of Greece Executive Committee Act 157/3/02.04.2019 | Adoption of the European Banking Authority's guidelines on the reporting of major events under Directive 2015/2366/EU
- Bank of Greece Act of the Executive Committee 164/2/13.12.2019 | Terms and conditions for: a) the authorisation of the establishment and operation of payment institutions and electronic money institutions in Greece and other provisions

Guidelines

- Bank of -Greece | Procedure for assessing requests to exempt providers from the emergency mechanism
- Bank of Greece | Specification of the data properties of the JSON file with the content of the EBA PSD2 Register
- 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
- 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

- Bank of Greece
- European Banking Authority - EBA

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.

Greece has implemented a range of initiatives to support SMEs and disadvantaged groups in leveraging digital technologies for trade. These measures include national strategies, funding programmes, and participation in EU-wide digital transformation efforts. The initiatives focus on providing financial support, enhancing digital skills, and improving access to digital infrastructure and services for SMEs across various sectors.

Summary

- The Digital Transformation Bible 2020-2025 serves as Greece's national strategy for digital transformation. This strategy outlines specific interventions aimed at supporting the digital transformation and strengthening the digital capacities of SMEs. In 2021, the Greek government introduced Greece 2.0, the country's recovery and resilience plan, as part of the European Union's Next Generation EU economic recovery package. This plan encompasses several initiatives designed to enable Greek SMEs to compete in the digital economy. Beyond the Digital Transformation Bible, in 2023, the Greek government published an updated Greek National Digital Decade Strategic Roadmap, which implements the European Union's Digital Decade Policy Programme 2030. This roadmap sets a target for over 90% of SMEs to attain a "basic level" of digital intensity by 2030.

- Under the Greece 2.0 framework, the government launched the Digital Transformation of SMEs programme with a budget of approximately USD 415 million. This programme provides financial support to SMEs for the purchase and adoption of digital technologies and related services. Additionally, the recovery and resilience plan includes provisions for tax incentives to facilitate SMEs' investments in digital technologies and the digitalisation of processes.

- As part of Greece 2.0, the Greek government established an agreement with the European Investment Fund. This agreement enables Greek SMEs to access funding for digital technology adoption through the European Investment Fund's Innovation and Digitalisation Portfolio Guarantee programme. The government also offers financial support to support digitalisation initiatives specifically in the agricultural sector under Greece 2.0.

- Greek SMEs benefit from the Digital Europe programme, which aims to increase access to digital skills training and improve data infrastructure. This initiative includes funding for a network of European Digital Innovation Hubs in Greece. These hubs function as "one-stop shops" to assist SMEs with digitalisation-related inquiries, allowing them to test new services or applications before investing and offering skills training to advance digital capabilities.

- As members of the European Union, Greek SMEs and minority-owned businesses can access various EU-wide programmes designed to enhance competitiveness in the digital economy. These programmes encompass financial support schemes, digital skills programmes for entrepreneurs, and regulatory support initiatives.

SOURCES

- Digital Transformation Bible 2020-2025
- Greek National Digital Decade Strategic Roadmap
- Greece 2.0 - National Recovery and Resilience Plan
- Greece 2.0: Digital Transformation of the Agri-Food Sector (measure ID 16653)
- Greece 2.0: Establishment of a digital business ecosystem and introduction of tax incentives for the facilitation of the SMEs digital transformation (measure ID 16973)
- Digital Transformation of Small and Medium Enterprises
- European Investment Fund: EIB Group and Greece take next steps in implementing RRF investments
- European Commission: European Union Digital Decade Policy Programme 2030
- European Commission: European Digital Innovation Hubs of Greece

02
Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Greece's digital economy across four key dimensions: digital economy size and activities, digital infra-structure and connectivity, digital skills, and digital government.

Size and Activities of the Digital Economy

To describe the size and activities of Greece'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 12.43% of Greece's imports. The share of advanced technology products in exports was lower at 7.51%, indicating a moderate technology trade imbalance.

Figure 1:
Telecommunications, Computer, Information and Audiovisual Services.

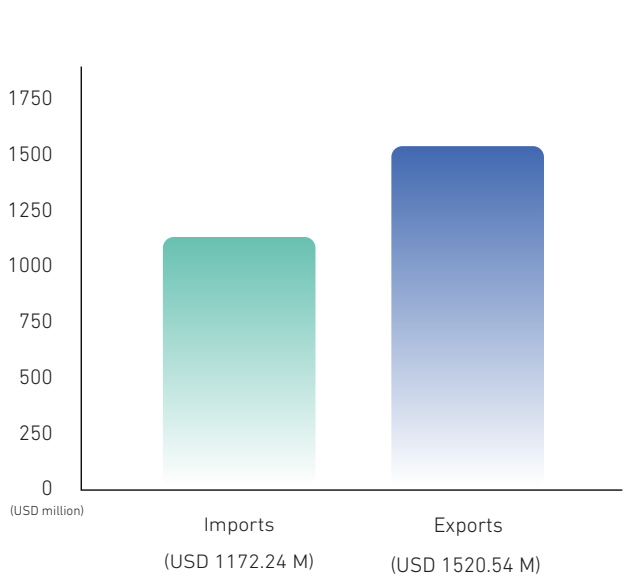


Figure 1 provides data for Greece's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2:
Digital Delivered Services

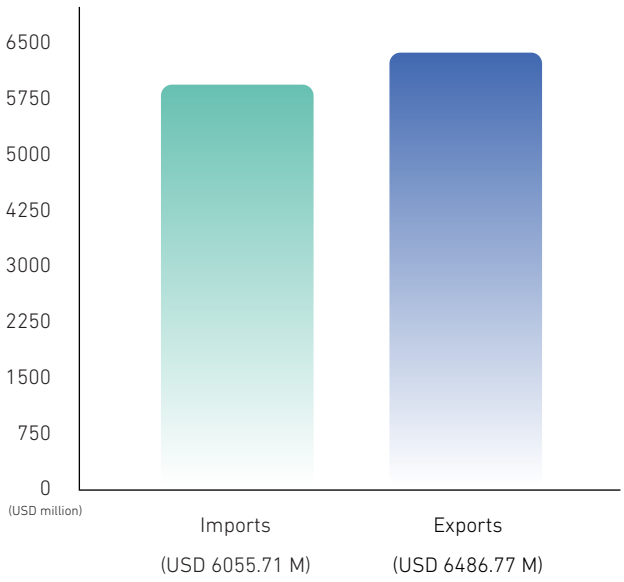


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity

To analyze Greece'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

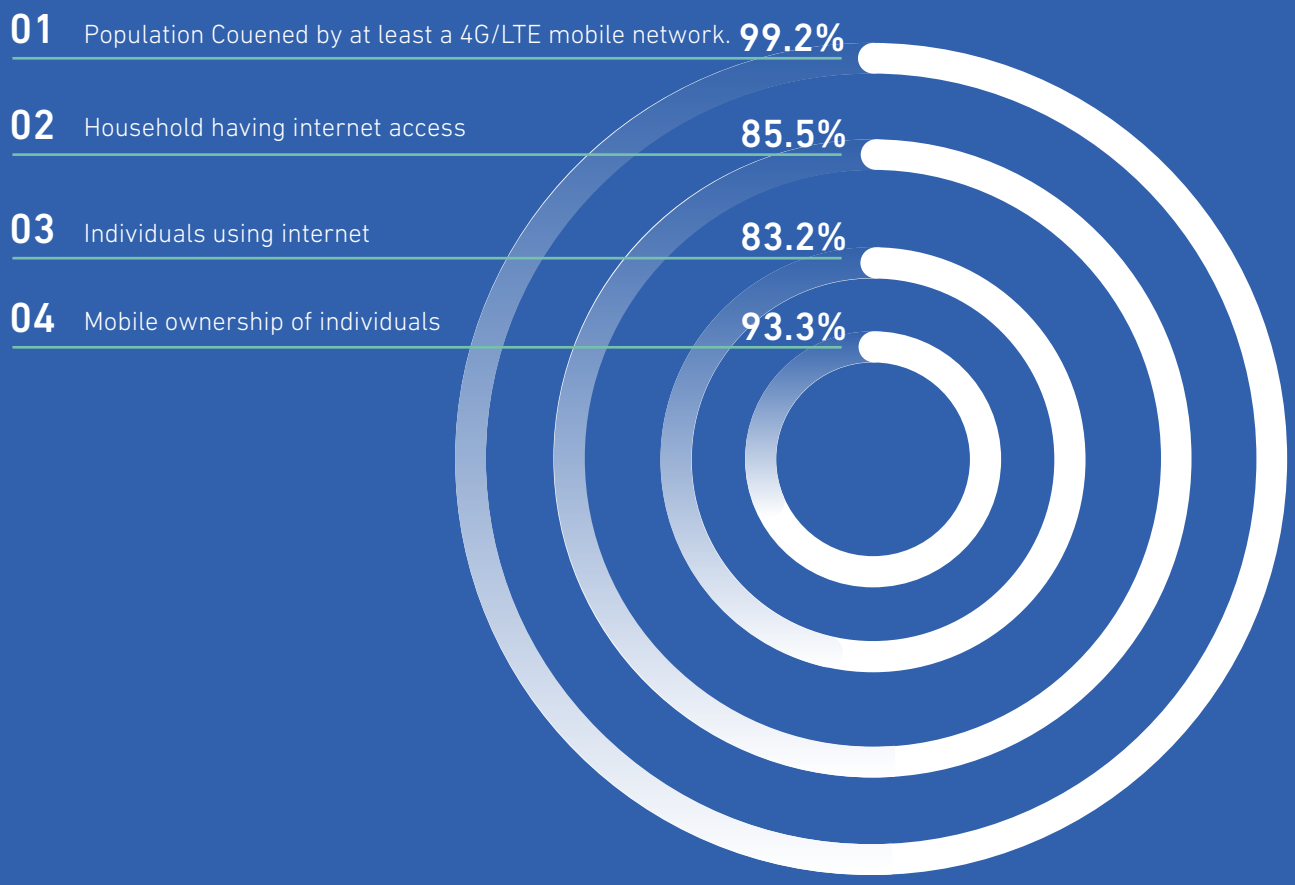
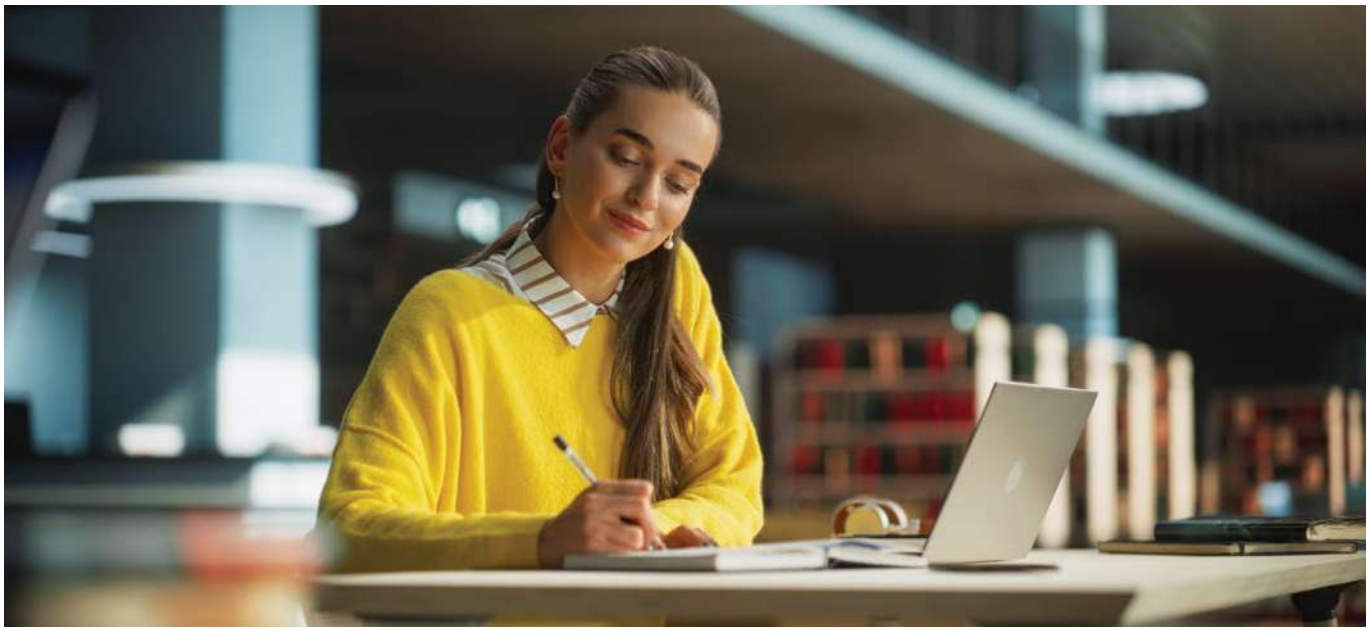


Figure 3 provides data to analyze Greece's digital infrastructure and connectivity in 2022.



Digital Skills

To document Greece'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 Greece was **93.06%** in 2021. Gross tertiary education enrollment ratio stood at **166.67%** in 2022, indicating exceptionally high participation in higher education. The adult literacy rate was **94%** in 2009. Government expenditure on education as a percentage of GDP was **2.91%** in 2022.

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

60.77%
were able to copy or move a file or folder (2019)

30.37%
had created electronic presentations with presentation software (2021)

40.61%
could find, download, install and configure software (2021)

Digital Government

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

In terms of digital government services in 2022, Greece had an operational government cloud platform in use. It had implemented a government interoperability framework. It had an advisory/R&D government open-source software policy. Greece maintained both an open government portal and an open data portal. Regarding institutional frameworks for digital government in 2022, Greece 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. Greece had institutionalized a whole-of-government approach to public sector digital transformation.

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

01 It had a current government technology or digital transformation strategy

02 It had either a strategy or program to improve digital skills in the public sector

03 It had either a strategy or 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 Greece and explain in which fora it engages in. 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 whether it is binding and which policy area(s) it can impact. Regarding international fora, we analyse participation in discussions at the pluri- and multilateral level.

Commitments

Free Trade Agreements

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

Conventions

Greece is party to the following conventions and agreements:

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

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

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

04 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)

05 Council of Europe Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (Cybersecurity)

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

07 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)

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

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

Greece 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)

03 United Nations draft Resolution A/78/L.49 on Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (Artificial Intelligence)

Greece 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)

Greece is a member state of the Organisation for Economic Co-operation and Development (OECD), which has adopted the following frameworks:

01 OECD Recommendation of the Council on Open Government (Open Government Data)

02 OECD Recommendation of the Council on Digital Security of Critical Activities (Cybersecurity)

03 OECD Recommendation of the Council on Artificial Intelligence (Artificial Intelligence)

04 OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information (Open Government Data)

05 OECD Recommendation of the Council concerning Guidelines for Cryptography Policy (Cybersecurity)

06 OECD Privacy Guidelines (Data Protection)

07 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (Consumer Protection)

08 OECD Digital Security Risk Management for Economic and Social Prosperity: Recommendation and Companion Document (Cybersecurity)

09 OECD Artificial Intelligence Principles (Artificial Intelligence)

10 OECD Declaration on Transborder Data Flows (Data Transfers)

Models

Greece has not adopted or been influenced by any model frameworks.

Other Commitments

- Greece 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, Greece is a participant in the Joint Statement Initiative which has finalised a stabilised text on the Agreement on Electronic Commerce on 26 July 2024.
- Greece is a member state of the European Union that participates in the Global Partnership on Artificial Intelligence. (Artificial Intelligence)
- Greece is party to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. (Cybersecurity)
- Additionally, Greece is a member state of the European Union that participates in the Hiroshima AI Process Friends Group (Artificial Intelligence).

Greece 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

Greece participates in the United Nations Global Digital Compact. (Cross-cutting)

@dcorg | www.dco.org