ASSEMBLY OF THE REPUBLIC

Law No. 46/2018
Of 13 August

Establishes the legal framework for cybersecurity, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The Assembly of the Republic decrees, under the terms of paragraph c) of article 161 of the Constitution, the following:

CHAPTER I
General Provisions

Article 1
Object

This law establishes the legal framework for cybersecurity, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Article 2
Scope

1 — This law shall apply to:

a) The Public Administration;
b) The Critical infrastructure operators;
c) The Operators of essential services;
d) The Digital service providers;
e) Any other entities using network and information systems.

2 — For the purposes of this law, the Public Administration shall include:

a) The State;
b) The autonomous regions;
c) The local authorities;
d) The independent administrative entities;
e) The public institutes;
f) The public companies;
g) The public associations.

3 — This law shall apply to digital service providers that have their main establishment in the national territory or, if not, appoint a representative established in national territory, that provides digital services thereof.

4 — For the purposes of the preceding paragraph, a digital service provider shall be deemed to have its main establishment in the national territory when its head office is located thereof.

5 — If an entity is simultaneously framed by more than one of sub-paragraphs a) to c) of n. º 1, the regime that results in the most demanding security level of the network and information systems shall apply.

6 — This law shall not apply to:

a) Network and information systems directly related to the command and control of the Armed Forces General Staff and branches of the Armed Forces;
b) Network and information systems processing classified information.

7 — The provisions of this law are without prejudice to compliance with the applicable legislation on:

a) The protection of personal data, in particular the provisions of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) and Law No. 26/2016 of 22 August;
b) The identification and designation of national and European critical infrastructures, namely Decree-Law No. 62/2011 of 9 May;
c) The fight against child sexual abuse and exploitation and child pornography, namely Law No. 103/2015, of 24 August;
d) The protection of users of essential public services, namely Law No. 23/96 of 26 July;
e) The security and emergency in the electronic communications industry, namely Law No. 5/2004 of 10 February.

8 — This law is without prejudice to the measures designed to safeguard the essential functions of the State, including the measures to protect information whose disclosure is contrary to national security interests, the maintenance of public order or to allow the investigation, detection and prosecution of criminal offenses.

Article 3
Definitions

For the purposes of this law, the following definitions apply:

a) «Computer security incident response team» means a team that acts by reference to a defined user community, representing an entity, providing a set of security services including, inter alia, the handling and response service network and information system security incidents;
b) «Technical specification» a document that sets the technical requirements that a product, process, service or system have to be compliant with;
c) «Incident» an event having an actual adverse effect on the security of network and information systems;
d) «Critical infrastructure» a component, system or part of such infrastructure located on national territory which is essential for the maintenance of functions vital to society, health, safety and economic or social well-being and whose disruption or destruction has a significant impact because of the impossibility to continue to perform those functions;
e) «Standard» a technical specification adopted by a recognised standardisation entity, for repeated or continuous application, which observation is not mandatory;
f) «Critical infrastructure operator» a public or private entity that operates a critical infrastructure;
g) «Essential service operator» means any public or private entity that provides an essential service;

h) «Traffic exchange point» a network structure that allows the interconnection of more than two independent stand-alone systems to facilitate traffic exchange on the Internet;

i) «Digital service provider» a legal person that provides a digital service;

j) «Domain name system service provider» an entity that provides domain name system (DNS) services on the internet;

k) «Network and information system» any device or group of interconnected or associated devices, in which one or more, develops executing a program, the automatic processing of digital data as well as the electronic communications network which supports the communication between those and the set of computer data stored, processed, retrieved or transmitted by those devices for their functioning, use, protection and maintenance;

l) «Top-level domain name registry» an entity that administers and operates the register of internet domain names under a specific top-level domain;

m) «Representative of a digital service provider» any natural or legal person established within the European Union explicitly designated to act on behalf of a digital service provider not established there;

n) «Risk» a circumstance or an event identifiable within reason standards having a potential adverse effect on the security of network and information systems;

o) «Security of network and information systems» the capacity of network and information systems to be resilient, within a certain level of trust, to actions that compromise the confidentiality, the integrity, the availability, the authenticity, and the non-repudiation of the data stored, transmitted or processed or the connexed services offered by, or accessible via, those network and information systems;

p) «Cloud computing service» a digital service that enables access to a scalable and elastic pool of shareable computing resources;

q) «Online marketplace» a digital service that allows consumers or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

r) «Online search engine service» a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a query on any subject and returns links in which information related to the requested content can be found;

s) «Digital service» an electronic information society service provided at a distance, by electronic means;

t) «Essential service» an essential service for the maintenance of crucial societal or economic activities, which depends on network and information systems and on which the occurrence of an incident can have a significant disruptive effect on the provision of that service;

u) «Domain name system» (DNS) a hierarchical distributed naming system in a network which refers queries for domain names;

v) «Incident handling» all procedures that support the detection, analysis, containment and response on an incident

Article 4
National Cyberspace Security Strategy

1 — The National Cyberspace Security Strategy defines the framework, objectives and lines of action of the State in this area, in accordance with the national interest.

2 — The National Cyberspace Security Strategy shall be approved by resolution of the Council of Ministers, on a proposal from the Prime Minister, after hearing the Superior Council for Cyberspace Security.

CHAPTER II
Cyberspace Security Framework

Article 5
Superior Council for Cyberspace Security

1 — The Superior Council for Cyberspace Security is the Prime Minister's specific advisory body on cyberspace security.

2 — The Superior Council for Cyberspace Security has the following composition:

a) The member of the Government responsible for the cybersecurity area, who presides

b) The National Security Authority, who replaces the president in his absences and impediments;

c) The Secretary General of the Internal Security System;

d) The Secretary General of the Information System of the Portuguese Republic;

e) Two Deputies appointed by the Assembly of the Republic through the *D'Hondt* method;

f) The Director of the Security Intelligence Service;

g) The Director of the Defence Strategic Intelligence Service;

h) The Coordinator of the National Cybersecurity Centre;

i) The Ambassador for cyber-diplomacy;

j) A representative of the electoral administration;

k) The Chairman of the Governing Board of the Agency for the Administrative Modernization, Public Institute;

l) The Director General of the Tax and Customs Authority;

m) The Director of the Government Computer Network Management Centre;

n) The Chairman of the Governing Board of the Shared Services of the Public Administration, Public Institute;

o) The Director of Communications and Information Systems of the Armed Forces General Staff;

p) A representative of the National Internal Security Network;

q) The President of the Institute for the Financial Management and Justice Equipments, Public Institute;

r) The Director of the National Unit for Cybercrime and Technological Crime Deterrence of the Criminal Police;

s) A representative of the Public Prosecution Service appointed by the Attorney General;

t) The President of the Foundation for Science and Technology, Public Institute;

u) The Director General of Education;

v) The Chairman of the Board of Directors of SPMS - Shared Services of the Health Ministry, Public State Company E.P.E.;

w) The Chairman of the Executive Board of Directors of the Infrastructures of Portugal, Limited Company;
x) The President of the Board of Directors of IAPMEI - Agency for Competitivity and Innovation, Public Institute;
y) The President of the Board of Directors of the National Communications Authority;
z) A representative of the Directorate of Natural Resources, Safety and Maritime Services;
aa) A representative of the National Network of Computer Security Incident Response Teams.

3 — The composition of the National Cybersecurity Council also includes a representative of the government of the Autonomous Region of the Azores and a representative of the government of the Autonomous Region of Madeira.

4 — The President, on his own initiative or at the request of any member of the Council, may convene other public bodies representatives or invite other participants with recognized merit to attend the meetings of the Superior Council for Cyberspace Security.

Article 6
Competences of the Superior Council for Cyberspace Security

1 — The National Cyberspace Security Council has the competence to:

a) Ensure the political-strategic coordination for cyberspace security;
b) Verify the implementation of the National Strategy for Cyberspace Security;
c) Issue an opinion on the National Strategy for Cyberspace Security prior to its submission for approval;
d) Prepare annually, or whenever necessary, an evaluation report on the implementation of the National Strategy for Cyberspace Security;
e) Propose to the Prime Minister, or to the Government member to whom he delegates powers, the approval of programmatic decisions related to the definition and execution of the National Strategy for Cyberspace Security;
f) Issue an opinion on cyberspace security matters;
g) Respond to requests from the Prime Minister, or the Government member to whom he delegates powers, within the scope of his powers.

2 — The annual report evaluating the implementation of the National Strategy for Cyberspace Security is sent to the Assembly of the Republic by 31 March of the year following that to which it relates.

Article 7
National Cybersecurity Centre

1 — The National Cybersecurity Centre operates under the National Security Office and is the National Cybersecurity Authority.

2 — The National Cybersecurity Centre's mission is to ensure that the country uses the cyberspace in a free, reliable and secure manner, by promoting the continuous improvement of the national cybersecurity and international cooperation, in articulation with all relevant authorities, as well as defining and implementing the measures and instruments necessary for anticipating, detecting, reacting and recovering situations which, in the imminence or occurrence of incidents, impair the national interest, the functioning of the Public Administration, the critical infrastructure operators, the operators of essential services and the digital service providers.

3 — The National Cybersecurity Centre is the single national contact point for the purposes of international cooperation, without prejudice to the legal duties of the Criminal Police regarding international cooperation in criminal matters.

4 — The National Cybersecurity Centre exerts regulatory, governing, supervisory, controlling and sanctioning functions in accordance with its competences.

5 — The National Cybersecurity Centre has the powers to issue cybersecurity instructions and to set the national cybersecurity alert level.

6 — Any legal provision regarding cybersecurity requires the prior opinion of the National Cybersecurity Centre.

7 — The National Cybersecurity Centre operates in articulation and close cooperation with the national structures responsible for cyber espionage, cyber defence, cybercrime and cyber terrorism and shall report to the competent authority, as soon as possible, the facts of which it is aware concerning the preparation and execution of crimes.

8 — The National Cybersecurity Centre operates in articulation with the National Data Protection Commission on incidents that cause the violation of personal data.

9 — The National Cybersecurity Centre may request any public or private entities for any collaboration or assistance it deems necessary for the exercise of its activities.

Article 8
National Computer Security Incident Response Team

1 — The National Computer Security Incident Response Team is the «CERT.PT».
2 — The «CERT.PT» functions in the National Cybersecurity Centre.

Article 9
Competences of the 'CERT.PT'

The «CERT.PT» has the following competences:

a) Exercise the operational coordination for incident handling, in particular in articulation with existing sectoral computer security incident response teams;
b) Monitor incidents with national implications;
c) Activate quick alert mechanisms;
d) Intervene in the reaction, analysis and mitigation of incidents;
e) Perform a dynamic risk analysis;
f) Ensure the cooperation with public and private entities;
g) Promote the adoption and use of common or standard practices;

h) Participate in national cooperation *fora* for computer security incident response teams;
i) Ensure the national representation in international cooperation *fora* of computer security incident response teams;
j) Participate in national and international training events.

Article 10
Operators of Essential Services

Operators of essential services are in the set of the types of entities operating in the sectors and subsectors listed in the annex to this law, which it integrates.

Article 11
Digital Service Providers

Digital service providers render the following services:

a) Online market service;
b) Online search engine service;
c) Cloud computing service.

CHAPTER III
Network and information system security

Article 12
Definition of security requirements and standardization

1 — The security requirements are defined in accordance with the provisions of the specific legislation, without prejudice to the provisions of article 18.

2 — The security requirements do not apply to:

a) Companies subject to the requirements of Articles 54-A to 54-G of the Electronic Communications Law, approved by Law No. 5/2004 of 10 February, as amended;
b) Trust service providers provided for in Article 19 of Regulation (EU) No. 910/2014 of 23 July of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

3 — Security requirements shall be defined to allow the use of internationally accepted standards and technical specifications applicable to the security of network and information systems, without imposing or discriminating in favour of the use of a particular type of technology.

Article 13
Definition of requirements for the notification of incidents

1 — The requirements for the notification of incidents are defined in accordance with the provisions of specific legislation, without prejudice to the provisions of article 19.

2 — The requirements for the notification of incidents do not apply to:

a) Companies subject to the requirements of Articles 54-A to 54-G of the Electronic Communications Law, approved by Law No. 5/2004 of 10 February, as amended;
b) Trust service providers provided for in Article 19 of Regulation (EU) No 910/2014 of 23 July of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Article 14
Security Requirements for the Public Administration and Operators of critical infrastructures

1 — The public administration and the Operators of critical infrastructures comply with the appropriate and proportionate technical and organizational measures to manage the risks on the security of the network and information systems they use.

2 — The measures provided for in the preceding paragraph shall ensure a level of security appropriate to the risk, taking into account the most recent technical developments.

3 — The Public Administration and the operators of critical infrastructures take appropriate measures to prevent incidents that affect the security of the network and information systems used and to minimize their impact.

Article 15
Notification of incidents for the Public Administration and operators of critical infrastructures

1 — The Public Administration and the operators of critical infrastructures notify the National Cybersecurity Centre on incidents with a relevant impact on the security of network and information systems within the time limit defined in the specific legislation referred to in article 13.

2 — The notification of operators of critical infrastructures includes information that enables the National Cybersecurity Centre to determine the crossborder impact of incidents.

3 — The notification does not entail additional responsibilities for the notifying party.

4 — In order to determine the relevance of the impact of an incident, the following parameters are considered:

a) The number of users affected;
b) The duration of the incident;
c) The geographical distribution regarding the area affected by the incident.

5 — When in the adequate circumstances, the National Cybersecurity Centre provides the notifying entity with relevant information concerning the follow-up of its notification, including information that may contribute to the effective handling of the incident.

6 — The National Cybersecurity Centre, after consulting the notifying entity, may disclose specific incidents in accordance with the public interest, safeguarding the security and interests of operators of critical infrastructures.

Article 16
Security Requirements for operators of essential services

1. The operators of essential services comply with the adequate and proportionate technical and organizational measures to manage the risks to the security of the network and information systems they use.

2 — The measures provided for in the preceding paragraph ensure a level of security adequate to the risk concerned, considering the most recent technical progresses.

3. The operators of essential services take the adequate measures to prevent incidents affecting the security of the network and information systems used to provide their essential services and to minimize the incidents impact ensuring the continuity of those services.

Article 17

Notification of incidents for operators of essential services

1 — The operators of essential services notify the National Cybersecurity Centre on incidents with a relevant impact on the continuity of the essential services they provide, within the time limit defined in the specific legislation referred to in article 13.

2 — The notification includes information that enables the National Cybersecurity Centre to determine the cross-border impact of incidents.

3 — The notification does not entail additional responsibilities for the notifying party.

4 — In order to determine the relevance of the impact of an incident, the following parameters are considered:

a) The number of users affected by the disruption of the essential service;
b) The duration of the incident;
c) The geographical distribution regarding the area affected by the incident.

5 — On the basis of the information provided in the notification, the National Cybersecurity Centre informs the single points of contact of the other affected Member States when the incident has an important impact on the continuity of the essential services in those Member States.

6 — In the case referred to in the preceding paragraph, the National Cybersecurity Centre safeguards the security and interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

7 — When in the adequate circumstances, the National Cybersecurity Centre provides the notifying operator of essential services with relevant information concerning the follow-up of its notification, including information that may contribute to the effective handling of the incident.

8 — The National Cybersecurity Centre forwards the notifications referred to in paragraph 1 to the single points of contact of the other affected Member States.

9 — The National Cybersecurity Centre, after consulting the notifying entity, can disclose information regarding specific incidents in accordance with the public interest.

10 — If an operator of essential services relies on a third-party digital service provider for the provision of an essential service, it notifies all the important impacts on the continuity of its services resulting from incidents affecting the digital service provider.

Article 18

Security Requirements for digital service providers

1 — The digital service providers identify and take the adequate and proportionate technical and organizational measures to manage the risks to the security of the network and information systems they use in the context of the provision of digital services.

2 — The measures referred to in the preceding paragraph ensure a level of security of the network and information systems appropriate to the risk concerned, considering the most recent technical progresses, and the following factors:

a) Security of systems and installations;
b) Handling of incidents;
c) Management of business continuity;
d) Follow-up, audit and tests performed;
e) Compliance with international standards.

3 — The digital service providers take measures to prevent incidents that affect the security of their network and information systems and to minimize their impact on digital services to ensure the continuity of those services.

4 — This article does not apply to micro and small enterprises, as defined by Decree-Law No. 372/2007 of 6 November, as amended.

5 — The elements contained in paragraphs 1 to 3 are subject to the Implementing Regulations of the European Commission.

Article 19

Notification of incidents for digital service providers

1 — The digital service providers notify the National Cybersecurity Centre on incidents with a substantial impact on the provision of digital services, within the time limit defined in the specific legislation referred to in article 13.

2 — The notification referred to in the preceding paragraph includes information that enables the National Cybersecurity Centre to determine the importance of the cross-border impacts.

3 — The notification does not entail additional responsibilities for the notifying party.

4 — In order to determine whether the impact of an incident is substantial, the following parameters are considered:

a) The number of users affected by the incident, including users who depend on the service to provide their own services;
b) The duration of the incident;
c) The geographical distribution regarding the area affected by the incident;
d) The severity level of the disruption to the service's operation;
e) The extent of the impact on economic and societal activities.

5 — The obligation to notify an incident only applies if the digital service provider has access to the information necessary

to assess the impact of an incident as function of the factors referred to in paragraph 2 of the preceding article.

6 — If the incidents referred to in paragraph 1 concern two or more Member States, the National Cybersecurity Centre informs the single points of contact of the other affected Member States.

7 — In the case referred to in the preceding paragraph, the National Cybersecurity Centre safeguards the security and interests of the digital service provider.

8 — The National Cybersecurity Centre, after consulting the notifying entity, can disclose specific incidents in accordance with the public interest.

9 — This article shall not apply to micro and small enterprises, as defined by Decree-Law No. 372/2007, of 6 November, as amended.

10 — The elements set out in paragraphs 1 to 5 are subject to the Implementing Regulation of the European Commission.

Article 20
Voluntary notification of incidents

1 — Without prejudice on the obligation to notify incidents established in this law, any entity may voluntarily notify incidents that have a significant impact on the continuity of its services.

2 — Regarding the processing of voluntary notifications, the provisions of article 17 apply, with the necessary adaptations.

3 — The voluntary notification can not originate obligations on the notifying entity to which it would not have been subject if it had not done the notification.

CHAPTER IV
Supervision and sanctions

Article 21
Supervisory and sanctioning competences

The National Cybersecurity Centre has the competences to supervise and to enforce sanctions as provided for in this law.

Article 22
Administrative offenses

Infringements of the provisions of this law are deemed as administrative offenses pursuant to the following articles.

Article 23
Very serious infractions

1 — The following are deemed as serious infractions:

a) Failure to comply with the obligation to implement security requirements as provided for in Articles 14, 16 and 18;
b) Failure to comply with the cybersecurity instructions issued by the National Cybersecurity Centre as provided for in Article 7 (5).

2 — The administrative offenses referred to in the preceding paragraph are punished with an administrative sanction of € 5000 to € 25 000, in the case of a natural person, and from € 10 000 to € 50 000, in case of a legal person.

Article 24
Serious infractions

1 — The following are deemed as serious infractions:

a) Failure to comply with the obligation to notify the National Cybersecurity Centre of incidents as provided for in Articles 15, 17 and 19;
b) Failure to comply with the obligation to notify the National Cybersecurity Centre of the exercise of activity in the digital infrastructure sector as provided for in paragraph 3 of article 29;
c) Failure to notify the National Cybersecurity Centre of the identification as a digital service provider as provided for in Article 30.

2 — The offenses referred to in the preceding paragraph are punishable by administrative sanction of € 1000 to € 3000, in the case of a natural person, and of € 3000 to € 9000, in the case of a legal person.

Article 25
Negligence

Negligence is be punishable, with the minimum and maximum limits of fines being halved.

Article 26
Instructing the administrative offenses proceedings and application of sanctions

The National Cybersecurity Centre has the competence to instruct the administrative offenses proceedings and the head officer has the competence to apply the administrative sanctions.

Article 27
Product of the administrative sanctions

The product of the administrative sanctions reverts to:

a) 60% to the State;
b) 40% to the National Cybersecurity Centre.

Article 28
Subsidiary Regime

Regarding administrative offenses, in all matters not provided for in this law, the provisions of the general regime of administrative offenses applies.

CHAPTER V
Final provisions

Article 29
Identification of operators of essential services

1 — For the purpose of complying with this law, the National Cybersecurity Centre shall identify the operators of essential services by 9 November 2018.

2 — The identification referred to in the preceding paragraph is subject to an annual update.

3 — The entities of the digital infrastructures sector shall immediately inform the National Cybersecurity Centre of the exercise of their respective activities.

Article 30

Identification of digital service providers

1 — Digital service providers shall immediately inform the National Cybersecurity Centre of the exercise of their activity.

2 — The notification obligation referred to in the preceding paragraph does not apply to micro and small companies, as defined by Decree-Law No. 372/2007, of 6 November, as amended.

Article 31

Complementary legislation

1 — The security requirements provided for in paragraph 1 of article 14 and paragraph 1 of article 16 shall be defined in specific legislation within 150 days after the entry into force of this law.

2 — The incident notification requirements provided for in paragraph 1 of article 15, paragraph 1 of article 17 and paragraph 1 of article 19 shall be defined in specific legislation within 150 days after the entry into force of this law.

Article 32

Repeal Rule

Resolution of the Council of Ministers no. 115/2017 of 24 August is hereby repealed.

Article 33

Entry into force and effect

1 — This law shall enter into force on the day following its publication.

2 — Notwithstanding the preceding paragraph, the regimes resulting from articles 14 to 27 shall take effect six months after the entry into force of this law.

Approved on 18 July 2018.

The President of the Assembly of the Republic, *Eduardo Ferro Rodrigues*.

Enacted on 1 August 2018.

Publish.

The President of the Republic, MARCELO REBELO DE SOUSA.

Countersigned on 6 August 2018.

The Prime Minister, *António Luís Santos da Costa*.

ANNEX

(referred to in Article 10)

Essential service operator sectors, subsectors and entity types

Sector	Subsector	Type of entities
Energy	Electricity	Electricity undertakings which carry out the function of 'supply'
		Distribution system operators.
		Transmission system operators.
	Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage and transmission
	Gas	Supply undertakings
		Distribution system operators.
		Transmission system operators.
		Storage system operators.
		Liquid natural gas (LNG) system operators.
		Natural gas undertakings.
		Operators of natural gas refining and treatment facilities.
Transports	Air transport	Air carriers.
		Airport managing bodies, airports and entities operating ancillary installations contained within airports
		Traffic management control operators providing air traffic control services
	Rail transport	Infrastructure managers.
		Railway undertakings including operators of service facilities.
	Sea and inland waterway transport	Inland, sea and coastal passenger and freight water transport companies not including the individual vessels operated by those companies.
		Managing bodies of ports including their port facilities and entities operating works and equipment contained within ports.
		Operators of vessel traffic services.
	Road transport	Road authorities.
		Operators of Intelligent Transport Systems.
Banking	—	Credit institutions.
Financial Market Infrastructures	—	Operators of trading venues.
		Central counterparties.
Health	Health care facilities	Health care providers.
Supply and distribution of drinking water	—	Suppliers and distributors of water intended for human consumption but excluding distributors for which the distribution of water for human consumption is only part of their general activity of distributing other commodities and goods not considered essential services.
Digital infrastructures	—	Internet exchange points.
		Domain Name System (DNS) Service Providers.
		Top-level domain name registries.

111575121