PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

PL 298/XXIV/2024

2025.01.22

Justifications

This bill aims to authorise the Government to approve the Cybersecurity Legal Regime, transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December to ensure a high common level of cybersecurity across the Union.

The preservation of cybersecurity plays a crucial role in national and international security, in the functioning of the State and economic agents, as well as in building citizens' trust in the process of digital modernisation of the Public Administration.

The transposition into the digital environment of essential functions of institutional activities and the personal and professional lives of citizens justifies the strengthening of the cybersecurity regulatory and organisational framework, implemented in harmony with the entire area and in defence against common cyber threats.

This legislative initiative arises from the awareness not only of the pressing severity posed by multiple cyber threats, but also of the high disruptive potential of their hostile actions against digital assets. It is imperative to strengthen national capacity for the prevention of acts that may affect national security and interest, as well as the various functional and productive dynamics of Portuguese society.

In fact, given the notable increase in the quantity and sophistication of threats, as well as the increasing use of and dependence on

information and communication technologies by society as a whole, it is essential to ensure the generalisation of cybersecurity in the organisational culture of the Portuguese business fabric and in the entities, bodies, and services making up the Public Administration.

In fact, the increase in the occurrence of cybersecurity incidents may compromise the

security and national interest, endanger human life, cause financial losses and compromise the confidentiality, integrity, and availability of information, networks, and information systems of public administration, operators of critical infrastructure, operators of essential services and digital service providers.

In view of these threats and considering the provisions of the Directive to be transposed, the regime approved by the authorised Decree-Law by this draft law significantly expands the range of entities covered by the regime, prioritising, on the one hand, the generalisation of cybersecurity risk prevention, but graduating the regulatory requirement according to the size of the entity and the importance of its activity, as well as privileging the proportionality of the applicable measures. Its scope covers a significant part of the public administration, adapting the regime to the size and typology of the public entity concerned. It should also be noted that, as permitted by the Directive to be transposed, the regime approved by the authorised Decree-Law excludes from its scope public entities in the fields of national security, public security, defence and intelligence services.

Among the relevant aspects of the regime approved by the

authorised Decree-Law is also the deepening of three fundamental instruments for public cybersecurity policies: the National Cybersecurity Strategy, defining national cybersecurity priorities and strategic objectives; the National Plan for Crisis Response and Large-Scale Cybersecurity Incidents, regulating and improving the management of such incidents; and the National Cybersecurity Reference Framework, which will bring together and enable the dissemination of norms, standards and best practices in cybersecurity management.

Moreover, the institutional framework of the regime approved by the authorised Decree-Law is extended in relation to the previous regime, as required by the Directive to be transposed In this regard, the National Cybersecurity Centre (CNCS) strengthens its role as the national cybersecurity authority, with the establishment of ‘sectoral’ and ‘special’ supervisory authorities exercising supervision over specific sectors of the economy also being highlighted, thus ensuring stability in the supervision of each of the sectors covered, as well as alleviating the cross-cutting tasks entrusted to the CNCS.

At the inter-administrative level, the proposed model establishes an architecture of convergence, cooperation, and interoperability between the various national entities responsible for cybersecurity and internal and external security, promoting, in particular, the transversality of relevant information flows and the sharing of tactical contributions in incident response between the national entities responsible for cybersecurity, with a view to maximising Portuguese public capabilities for the prevention, early detection, mitigation, prosecution and accountability of cyber threats.

Draft Law No .....

Strengthening cooperation with the private sector is another of the axes of the institutional design provided for in the regime approved by the authorised Decree-Law, fostering collaboration between the competent authorities and the private sector **in the various** relevant matters.

As for the risk management model provided for in the regime approved by the authorised Decree-Law, it consists of the establishment of predefined risk standards applicable to each sector and type of entity, and the application of corresponding prevention measures, plus an analysis of the residual risk. This model relieves authorities of a case-by-case analysis of the risk of each covered entity, and facilitates covered entities in identifying the category to which they belong and, consequently, the minimum measures they must adopt. Accordingly, the proposed model introduces simplicity, predictability, and better alignment of mandatory measures with the threat framework applicable to each sector of activity. On the other hand, the model fosters the creation of a cybersecurity certification market, which will have economic utility and will allow for the generalisation of a presumption of conformity of entities.

Finally, as regards the supervisory model provided for in the regime approved by the authorised Decree-Law, this, reflecting the provisions of the Directive to be transposed, provides for a dual regime, differentiating the treatment to be given to essential and important entities according to the cybersecurity risks associated with each category, in compliance, once again, with the principle of proportionality.

Draft Law No .....

This Decree-Law focused, essentially, on the construction of the applicable legal regime on cybersecurity. However, the entry into force of the new regime will necessarily imply a significant strengthening of the capacity of the CNCS and a reflection on its institutional framework.

The regime provided for in this Decree-Law was subject to public consultation between 22 November and 12 December 2024. Specifically, the hearing of the governing bodies of the Autonomous Region of Madeira and the Autonomous Region of the Azores, the National Data Protection Commission, the National Communications Authority, the National Security Office, the National Cybersecurity Centre, the Internal Security System, the Secretary-General of the Information System of the Portuguese Republic, the National Emergency and Civil Protection Authority, the Bank of Portugal, the Securities Market Commission, the Supervisory Authority for Insurance and Pension Funds, the Ombudsman's Office, the Superior Council of the Judiciary, the Superior Council of Administrative and Tax Courts, the Superior Council of the Public Prosecutor's Office and the Attorney General's Office was raised.

Therefore:

In accordance with Article 197(1)(d) of the Constitution, the Government hereby submits the following draft Law to the Assembly of the Republic:

Article 1

Draft Law No .....

Subject

The Government is authorised to approve the Cybersecurity Legal Regime, transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, aimed at ensuring a high common level of cybersecurity across the Union.

Article 2

Meaning and scope

The authorisation referred to in the preceding Article shall have the following meaning and scope:

a) Approve the legal regime for cybersecurity**,** transposing into national law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 1 Directive), by:

i) The extension of the scope of the cybersecurity legal regime;

ii) The development of the structuring instruments of Cyberspace Security;

iii) The provision of a new institutional framework for cyberspace security;

iv) The provision of a new cybersecurity risk management framework;

v) Providing for a new cybersecurity incident prevention

and treatment regime;

vi) Providing for a new cybersecurity oversight and enforcement regime;

vii) Providing for a new cybersecurity sanctioning regime;

b) Implement, in its internal legal order, the obligations stemming from Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), by implementing a national cybersecurity certification framework;

c) To make the ninth amendment to the Internal Security Law, approved by Law No 53/2008 of 29 August, as amended by Law No 59/2015 of 24 June, by Decree-Law No 49/2017 of 24 May, by Laws No 21/2019 of 25 February and No 73/2021 of 12 November, by Decree-Law No 122/2021 of 30 December, by Law No 24/2022 of 16 December and by Decree-Laws No 41/2023 of 2 June and No 99-A/2023 of 27 October;

d) Carry out the second amendment to the Cybercrime Law, approved by Law No 109/2009 of 15 September, as a.ended by Law No 79/2021 of 24 November.

Article 3

Draft Law No .....

Duration

The duration of the authorisation granted by this Law shall be 180 days.

Seen and approved by the Council of Ministers of (...)

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

AUTHORISED DECREE-LAW

Preface

(…)

Therefore:

In the use of the legislative authorisation granted by Article […] of Law No […], of […], and in accordance with Article 198(1)(b) of the Constitution, the Government decrees the following:

Article 1

Subject

1 - This Decree-Law approves o **cybersecurity legal regime,** transposing into the national legal order Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 1 Directive).

2 - This Decree-Law also proceeds to:

a) The implementation in the internal legal order of the obligations stemming from Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013

(Cybersecurity Act), implementing a national cybersecurity certification framework;

b) Ninth amendment to the Internal Security Law, approved by Law No 53/2008 of 29 August, as amended by Law No 59/2015 of 24 June, by Decree-Law No 49/2017 of 24 May, by Laws No 21/2019 of 25 February and No 73/2021 of 12 November, by Decree-Law No 122/2021 of 30 December, by Law No 24/2022 of 16 December and by Decree-Laws No 41/2023 of 2 June and No 99-A/2023 of 27 October; and

c) Second amendment to the Cybercrime Law, approved by Law No 109/2009 of 15 September, as amended by Law No 79/2021 of 24 November.

3 - The provisions of this Decree-Law shall be without prejudice to the measures and legal regime in force to safeguard the essential functions of the State, in particular the measures and provisions relating to the preservation of security and the national interest, the production of information for the internal and external security of the Portuguese State, the protection of the State Secret and classified information, and to safeguard the maintenance of public order and to enable the investigation, detection and prosecution of criminal offences, without prejudice to Articles 6 and 7.

Article 2

Cybersecurity Legal Regime

Draft Law No .....

The Cybersecurity Legal Regime is hereby approved as an annex to this Decree-Law, of which it forms an integral part.

Article 3

Amendment to Law No 53/2008 of 29 August

Article 16 of the Internal Security Law, approved by Law No 53/2008 of 29 August, in its current wording, is replaced by the following:

'Article 16

[...]

1 - [...].

2 - [...].

3 - [...].

4 - The Secretary-General of the Internal Security System shall be responsible for convening, in accordance with Article 25A, a crisis office following the attribution of a high threat level by the Security Intelligence Service, or equivalent national cybersecurity alert level, or when informed by the National Cybersecurity Centre or any competent entity, including security forces and services, of the occurrence of a significant cyber threat or of a crisis or incident that could be considered large-scale.

Article 4

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Amendment to Law No 53/2008 of 29 August

Article 25-A is added to the Internal Security Law, approved by Law No 53/2008 of 29 August, in its current wording, as follows:

'Article 25a

Crisis Unit

1 - The crisis office referred to in Article 16(4) shall be composed of representatives of the Criminal Police, the Security Intelligence Service, the Strategic Defence Intelligence Service, the National Cybersecurity Centre and the Cyber Defence Operations Command, or other relevant entities.

2 - The purpose of the crisis office referred to in the previous paragraph is to ensure, in a coordinated manner and without prejudice to the powers legally conferred on each entity, the conduct of cybersecurity crises with an impact on internal security and, in situations of occurrences with a cross-border impact, to ensure functional interoperability with similar entities in the European Union.

Article 5

Amendment to Law No 109/2009 of 15 September

Article 2 of the Cybercrime Law, approved by Law No 109/2009 of 15 September, in its current wording, is replaced by the following:

Draft Law No .....

‘Article 2.

[…]

For the purposes of this Law, the following definitions shall apply:

a) […];

b) […];

c) […];

d) […];

e) […];

f) […];

g) […];

h) ‘Vulnerability’ means a fragility, susceptibility or failure, affecting network and information systems, information or communication technology products or services, that can be exploited by a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April.

Article 5

Addition to Law No 109/2009 of 15 September:

Article 8a is added to the Cybercrime Law, approved by Law No 109/2009 of 15 September, in its current wording, as follows:

Article 8a

Draft Law No .....

Acts not punishable in the public interest of cybersecurity

1 - Acts capable of constituting the offences of unlawful access and unlawful interception provided for in Articles 6 and 7 respectively shall not be punishable if the following circumstances are cumulatively present:

a) The agent acts with the sole intention of identifying the existence of vulnerabilities in information systems, information and communication technology products and services, which have not been created by him or by a third party on whom he relies, and with the purpose of contributing to the security of cyberspace by disclosing them;

b) The agent does not act with the intention of obtaining an economic advantage or promise of an economic advantage as a result of his action, without prejudice to the remuneration he receives in return for his professional activity;

c) The agent shall communicate, immediately after his or her action, any identified vulnerabilities to the owner or the person designated by him to manage the information system, product or service of information and communication technologies, to the holder of any data obtained and that are protected under the applicable legislation on the protection of personal data, namely the General Data Protection Regulation (GDPR), approved by Regulation (EU)

2016/679 of the European Parliament and of the Council of 27 April, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August and Law No 59/2019 of 8 August.

d) The action of the agent shall be proportionate to its purposes and strictly limited by them, being sufficient with the necessary actions to identify vulnerabilities and avoiding causing:

i) A disruption or interruption of the operation of the system or service concerned;

ii) Erasure or deterioration of computer data or unauthorised copying thereof;

iii) Any adverse, damaging, or harmful effect on the affected person or entity, directly or indirectly, or on any third party, excluding the effects corresponding to the illegitimate access or illegitimate interception itself, as provided for in Articles 6 and 7, as well as those that would already result, with a high probability, from the detected vulnerability itself or from its exploitation.

e) The action of the agent does not constitute a breach of personal data protected under the applicable legislation on the protection of personal data, namely Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April, Law No

Draft Law No .....

58/2019 of 8 August and Law No 59/2019 of 8 August.

2 - The communication provided for in point (c) of the preceding paragraph shall also be made to the national cybersecurity authority without undue delay.

3 - For the purposes of determining the proportionality of the action of the agent, it shall be taken into account whether it was necessary to detect the vulnerability and whether the extent of computer systems or data accessed, consulted and/or copied was imposed by the interest in contributing to the security of cyberspace, the use of the following practices being expressly prohibited:

a) Denial of service (DoS) or distributed denial of service (DDoS) mechanisms;

b) Social engineering, defined as the act of deceiving managers or users of information systems with a view to making sensitive or confidential information available;

c) Phishing and variants;

d) Theft or robbery of passwords or other sensitive information;

e) Wilful deletion or alteration of computer data;

f) Wilful damage to the information system;

g) Installation and distribution of malicious software.

4 - Without prejudice to applicable data protection rules,

computer data communicated to the owner or person in charge of managing the information system, information and communication technology product and service, or to the national cybersecurity authority, shall be deleted within 10 days from the moment the vulnerability is remedied, and its secret nature shall be ensured throughout the procedure.

5 - Acts committed with the consent of the owner or administrator of an information system, information and communication technology product or service shall also not be punishable, without prejudice to the duty to notify any vulnerabilities identified to the coordinating national authority in charge of responding to cybersecurity incidents any vulnerabilities identified, as provided for in the Cybersecurity Legal Regime.

Article 6

Repeal

The following are repealed:

a) Articles **59** to 65 and points (m) to (t) of Article 178(3) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, in its current wording;

b) The Cyberspace Security Legal Regime, approved by Law No 46/2018 of 13 August;

c) Regulation of the Cyberspace Security Legal Regime,

Draft Law No .....

approved by Decree-Law No 65/2021 of 30 July,

d) Article 2a of Decree-Law No 3/2012 of 16 January, as amended, approving the organisation of the National Security Office.

Article 7

Transitional Rule

1 - The entry into force of this Decree-Law shall not affect the validity of decisions taken by the Safety Assessment Committee under the previous regime, which shall continue to produce effects for a period of 180 days after the date of entry into force of this Decree-Law, during which a new safety assessment shall be carried out.

2 - On the basis of the new security assessment referred to in the preceding paragraph, and under the regime approved as an annex to this Decree-Law, the Member of the Government responsible for cybersecurity may decide to renew, modify or replace the decisions adopted by the Security Assessment Committee under the previous regime.

Article 8

Effective date

Articles 27 to 30, 33, and 63(1)(a) and (b) of the Cybersecurity Legal Regime approved in the Annex to this Decree-Law, of which it forms

an integral part, shall take effect 18 months after the publication of the regulations referred to in Articles 8, 14, 26, 31, 32 and 83 of that regime.

Article 9

Entering into force

This Decree-Law shall enter into force 90 days after its publication.

Seen and approved by the Council of Ministers of

The Prime Minister

The Minister for the Presidency

(…)

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

ANNEX

(referred to in Article 2)

Cybersecurity Legal Regime

CHAPTER I

General provisions

Article 1

Subject

1 - This Decree-Law establishes the Cybersecurity Legal Regime, transposing into national law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 1 Directive).

2 - The provisions of this Decree-Law shall be without prejudice to compliance with the provisions of the applicable legislation on:

a) Criminal investigation proceedings by the competent judicial authorities and criminal police bodies, in particular the Public Prosecutor’s Office and the Criminal Police;
b) Processes falling within the exclusive competence of the Security Intelligence Service and the Strategic Defence Intelligence Service in relation to the production of information relating to the safeguarding of national

independence, national interests, the external and internal security of the Portuguese State, and the prevention of sabotage, terrorism, espionage and the commission of acts which, by their nature, may alter or destroy the constitutionally established rule of law;

a) Protection of personal data, in particular within the scope of the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August, and Law No 59/2019 of 8 August;

b) Identification and designation of national and European critical infrastructures, in particular under Decree-Law No 20/2022 of 28 January;

c) Combating the sexual abuse and sexual exploitation of children and child pornography, in particular under Law No 103/2015 of 24 August;

d) Protection of users of essential public services, in particular under the Electronic Communications Law, approved by Law No 23/96 of 26 July, as amended;

e) Security and emergency in the electronic communications sector, in particular under the provisions of Law No 16/2022 of 16 August, as amended;

f) State Secrets and Classified Information, in particular under the provisions of Organic Law No 2/2014 of 6 August, as amended.

Article 2

Draft Law No .....

Definitions

For the purposes of this Decree-Law, the following shall mean:

a) 'Asset' means any information and communication system, equipment and other physical and logical resources managed or owned by the entity that support, directly or indirectly, one or more services.

b) 'Competent cybersecurity authority' means the National Cybersecurity Centre (CNCS) or, where applicable, the competent national sectoral cybersecurity authority pursuant to point (a) of Article 15(2) of this Decree-Law, without prejudice to the reservations of exclusive competence of public entities with responsibilities for criminal investigation, intelligence generation and cyber defence;

c) Cyber threat' means a cyber threat as defined in point 8 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;

d) 'Significant cyber threat' means a cyber threat that, based on its technical characteristics, can be considered likely to have a serious impact on the network and information systems of an entity or users of the entities' services, causing considerable material or immaterial damage;

e) 'Cybersecurity' means cybersecurity as defined in point 1 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;

f) 'Entity' means a legal person created and recognised as

such under the national law of its place of establishment, which, acting in its own name, may exercise rights and be subject to obligations;

g) 'Entities competent in the field of cyberspace security' means the Cyber Defence Command of the General Staff of the Armed Forces, the Judicial Police, the Security Intelligence Service and the Strategic Defence Intelligence Service;

h) 'Entity providing domain name registration services' means a registrar or an agent acting on behalf of registrars, such as a provider or reseller of privacy protection or intermediary server registration services;

i) 'Technical specification' means a technical specification as defined in point 4 of Article 2 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October;

j) 'Incident' means an event that jeopardises the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or of services offered by or accessible via network and information systems;

k) 'Large-scale cybersecurity crisis of incident', means an incident that causes a level of disruption exceeding the capacity of the Portuguese State to respond, that has a significant impact on at least two Member States of the European Union, or that, due to its scope and systemic impact, calls for urgent intersectoral coordination;

l) 'Significant incident' means an incident that:

i) Causes, or is likely to cause, serious operational disruptions of services or financial losses to the entity concerned;

ii) Affects, or is likely to affect, other natural or legal persons by causing considerable material or non-material damage.

m) 'Risk matrix' means the reference framework establishing the risk values for the set of risk scenarios affecting a sector and subsector of activity, considering common assets, key threats and vulnerabilities;

n) 'Cybersecurity risk management measures or cybersecurity measures' means technical, operational and organisational measures aimed at managing the risks posed to the security of network and information systems that they use in their operations or in the provision of their services, as well as preventing or minimising the impact of incidents on recipients of their services and on other services;

o) 'Online marketplace' means an online marketplace as referred to in Article 3(n) of Decree-Law No 57/2008 of 26 March, as amended, laying down the rules applicable to unfair commercial practices;

p) 'Online search engine' means an online search engine as defined in point (5) of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council of

20 June, and point (j) of Article 3 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October;

q) 'Standard' means a standard as referred to in Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October;

r) 'Cybersecurity operations' means actions to operationalise cybersecurity risk management measures;

s) 'Research organisation' means an entity whose primary purpose is to carry out applied research or experimental development with a view to exploiting the results of such research for commercial purposes, excluding educational establishments;

t) 'Social media service platform' means an online platform, defined in accordance with point (i) of Article 3 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October, that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular through conversations, publications, videos and recommendations;

u) 'Traffic exchange point' means a network structure that:

i) Allows the interconnection of more than two independent networks (autonomous systems), in particular in order to facilitate the exchange of Internet traffic;

ii) Only interconnect autonomous systems;

iii) Does not imply that internet traffic between a pair of participating autonomous systems passes through, alters or otherwise interferes with a third autonomous system.

v) 'DNS service provider' means an entity that provides publicly available recursive domain name resolution services for internet end-users or resolution services with authority for domain names for use by third parties, with the exception of root name servers;

w) 'Trust service provider' means a trust service provider as defined in point 19 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April;

x) 'Managed security service provider' means a managed service provider that performs or assists in activities related to the management of cybersecurity risks;

y) 'Managed service provider' means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructures, applications or any other network and information systems, through assistance or active administration performed at customer premises or remotely;

z) 'Qualified trust service provider' means a qualified trust service provider as referred to in point 20 of Article 3 of

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April;

aa) 'ICT process' means an ICT process as defined in point 14 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;

bb) 'ICT product' means an ICT product as defined in point (12) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;

cc) 'Near miss' means an event that could have jeopardised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems, but which was avoided or did not materialise;

dd) 'Content delivery network' means a network of servers distributed geographically for the purpose of ensuring the high availability, accessibility or rapid distribution of digital content and services to internet users on behalf of content and service providers;

ee) 'Registration of top-level domain names' or 'Registration of TLD (Top Level Domain)' names means an entity to which a specific TLD has been delegated and which is responsible for its administration, including the registration of domain names under the TLD and the technical operation of that

TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files to name servers, irrespective of whether any of these operations are performed by the entity itself or are outsourced, but excluding situations where the names of the TLD are used by a registry for its own use only;

ff) 'Public electronic communications network' means a public electronic communications network within the meaning of point (oo) of Article 3(1) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended;

gg) 'Networks and information systems' means:

i) An electronic communications network, pursuant to point (mm) of Article 3(1) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended;

ii) A device or group of interconnected or associated devices, one or more of which perform automatic processing of digital data on the basis of a program; or

iii) Digital data stored, processed, obtained or transmitted by elements referred to in points (i) and (ii) for the purpose of their operation, use, protection and maintenance;

hh) 'Representative' means any natural or legal person, established in the European Union, expressly designated to

act on behalf of a DNS service provider, a Top Level Domain Name Registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, a provider of online marketplaces, online search engines or social media service platforms that is not established in the European Union, who can be contacted by the competent entities, instead of the entity represented, in relation to the latter's obligations under this Decree-Law;

ii) 'Risk', the extent of the possibility of a loss or disruption caused by an incident, resulting from the combination of the magnitude of such loss or disruption and the probability of the occurrence of the incident;

jj) 'Residual risk' means a risk measure that exists after the adoption of the minimum cybersecurity measures;

kk) 'Security of network and information systems' means the ability of network and information systems to withstand, at a given level of confidence, events that may jeopardise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those networks and information systems;

ll) 'Data centre service' means a service comprising structures or groups of structures dedicated to the hosting, interconnection and centralised operation of network and IT

equipment providing data storage, processing and transmission services, together with all facilities and infrastructures for energy distribution and environmental control;

mm) 'Cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and adaptable pool of shareable computing resources, including where those resources are distributed across multiple locations;

nn) 'Electronic communications service' means an electronic communications service pursuant to point (ss) of Article 3 of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended;

oo) 'Trust service' means a trust service as defined in point 16 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April;

pp) 'Qualified trust service' means a qualified trust service as defined in Article 3(17) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament

and of the Council of 11 April;

qq) 'ICT service' means an ICT service as defined in point (13) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;

rr) 'Domain name system' or 'DNS' means a hierarchically distributed name system that enables the identification of services and resources on the Internet, allowing end-user devices to use internet routing and connectivity services to access those services and resources;

ss) 'Digital service' means a service within the meaning of Article 3(g) of Decree-Law No 30/2020 of 29 June laying down the rules governing the information procedure in the field of technical rules on products and rules on information society services;

tt) 'Incident handling' means all actions and procedures aimed at preventing, detecting, analysing, containing or responding to an incident and recovering from an incident;

uu) 'Vulnerability' means a fragility, susceptibility or failure, affecting network and information systems, information or communication technology (ICT) products or services, that can be exploited by a cyber threat.

Article 3

Subjective scope

1 - This Decree-Law shall apply to private entities of one of the types listed in Annexes I or II to this Decree-Law which,

respecting the territorial scope criteria set out in the following Article:

a) Are qualified as medium-sized enterprises in accordance with Article 2 of Annex III to this Decree-Law, corresponding to that provided for in Commission Recommendation 2003/361/EC of 6 May, or exceed the thresholds for medium-sized enterprises provided for in paragraph 1 of that Article; and

b) Provide their services or carry out their activities in the European Union.

2 - This Decree-Law shall also apply to entities of one of the types listed in Annexes I or II to this Decree-Law which, irrespective of their nature and size and in compliance with the territorial scope criteria laid down in the following Article, meet at least one of the following requirements:

a) The entity concerned is:

i) A provider of public electronic communications networks or provider of publicly available electronic communications services;

ii) A trust service provider;

iii) Top-level domain name registration, domain name registration service provider, and domain name system service provider.

b) The entity concerned is the only provider of a service that is essential for the maintenance of critical social or economic

activities, including activities corresponding to the sectors, subsectors and types of entities referred to in Annexes I and II to this Decree-Law;

c) A disruption of the service it provides could significantly affect public security, public protection or public health;

d) A disruption of the service it provides may generate considerable systemic risks, especially for sectors for which such disruption may have a cross-border impact;

e) The entity is critical due to its specific importance, at national or regional level, for the sector or type of service concerned, or for other interdependent sectors.

3 - This Decree-Law applies to the Public Administration, covering:

a) Direct State administration services, central and peripheral;

b) Direct administration services of the Autonomous Regions, central and peripheral;

c) Entities of the indirect administration of the State;

d) Indirect administration entities of the Autonomous Regions;

e) Self-governing entities;

f) Independent administrative bodies and entities, with the exception of the Banco de Portugal, the Securities Market Commission, and the Insurance and Pension Funds Supervisory Authority.

4 - This Decree-Law shall apply to the following entities:

a) Ombudsman;

b) Economic and Social Council;

c) Technical and administrative services of the Presidency of the Republic, the Assembly of the Republic, the Courts and secretariats with competence for the processing of procedures, the High Council of the Judiciary, the High Council of Administrative and Fiscal Courts, and the High Council of the Public Prosecution Service, without prejudice to (6).

5 - This Decree-Law shall apply to entities that, irrespective of their size, are identified as critical entities pursuant to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December on the resilience of critical entities, without prejudice to (3)(f).

6 - This Decree-Law shall not apply:

a) To the General Staff of the Armed Forces and of the branches of the Armed Forces, as regards network and information systems directly related to their command and control;

b) To public entities with criminal investigation responsibilities and criminal police and public security bodies, as regards network and information systems directly related to their command and control;

c) To public entities with exclusive responsibilities for the production of information, in particular the Information System of the Portuguese Republic, the Strategic Defence Information Service, and the Security Intelligence Service,

as regards network and information systems directly related to their command and control;

d) To public entities whose activity concerns network and information systems directly related to the production and dissemination of classified information, including national, NATO, and European Union trademarks, or catalogued as a State Secret, with regard to such network and information systems;

e) To other public entities operating in the fields of national security, public security, defence, and intelligence with regard to network and information systems directly related to the activities of intelligence generation and the prevention, investigation, detection and prosecution of criminal offences;

f) Private entities providing services exclusively to one or more of the entities referred to in the preceding points and in respect of these activities.

7 - This Decree-Law shall apply to the entities referred to in Article 15(2)(b) only as regards the exercise of their competences as special national cybersecurity authorities.

8 - This Decree-Law is without prejudice to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December on digital operational resilience for the financial sector.

Draft Law No .....

Article 4

Territorial delimitation of the subjective scope

1 - This Decree-Law shall apply to the entities referred to in (1) and (2) of the preceding Article which:

a) Have an establishment in the national territory;

b) In the case of undertakings providing public electronic communications networks or publicly available electronic communications services, make them available in the national territory;

c) For domain name system service providers, top-level domain name registration, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms:

i) Have their principal place of establishment in the national territory;

ii) Having no establishment in the European Union, his representative has an establishment in the national territory.

2 - For the purposes of (c)(i) of the preceding paragraph, the entity shall be deemed to have its principal place of business in the national territory when:

a) Decisions related to cybersecurity risk management measures are predominantly taken on national territory;

b) Cybersecurity operations are carried out on national territory, if it is not possible to determine whether decisions related to cybersecurity risk management measures were taken there predominantly or in another Member State of the European Union.

c) The establishment of the entity with the highest number of employees is located in the national territory, if it is not possible to determine whether cybersecurity operations are carried out there.

3 - In accordance with Article 20, the CNCS, upon a request for mutual assistance from another Member State of the European Union and in relation to an entity referred to in (1)(c), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned.

Article 5

Extraterritorial scope

1 - In order to prevent significant cyber threats to the security of network and information systems of a large number of users, the CNCS may, after consulting the Supreme Cybersecurity Council, adopt corrective or restrictive enforcement measures, including the order to suspend the service in the national territory, addressed to a service provider without establishment or representation in the national territory that does not offer

appropriate cybersecurity measures.

2 - Except where the measures are urgent, the CNCS shall provide a preliminary statement of reasons for the decisions to the service provider, granting a time limit for reply of no less than 10 days.

3 - For the purposes of determining and substantiating the implementing measures provided for in the preceding paragraphs, the CNCS shall take into account the actions and measures, as well as their effectiveness and extent, taken by European and international cybersecurity authorities.

4 - The competent cybersecurity authority, in accordance with its competences and to the extent necessary, may, in relation to an entity with a relevant connection to the national territory, assist the competent authorities of the Member States of the European Union, upon their reasoned request, in particular by:

a) Providing information regarding a supervisory or enforcement measure taken in relation to that entity through its Single Point of Contact;

b) The application of supervisory or enforcement measures in accordance with Chapter VI, where necessary together with the competent authority of the respective Member State of the European Union;

c) Providing support to the competent authority of the respective Member State of the European Union with regard to the application by the latter of supervisory or enforcement measures, which may include the forms of

assistance referred to in the previous points.

5 - The competent cybersecurity authority may refuse the assistance requested in accordance with the preceding paragraph only if it exceeds its powers, is disproportionate to its supervisory functions or compromises essential interests of the Portuguese State in terms of national security, public security or defence.

Article 6

Essential entities and important entities

1 - For the purposes of this Decree-Law, the following shall be considered essential entities:

a) Entities of one of the types referred to in Annex I to this Decree-Law that exceed the thresholds for medium-sized enterprises provided for in Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May;

b) Providers of qualified trust services and top-level domain name registration, and providers of domain name systems, regardless of their size;

c) Undertakings providing public electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises in accordance with Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation

2003/361/EC of 6 May;

d) Public Administration entities whose tasks include the provision of services in the areas of development, maintenance, and management of information and communication technology infrastructures, or those with a particularly high degree of digital integration in the provision of their services, identified and qualified in accordance with Article 8;

e) Entities identified as critical entities pursuant to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December on the resilience of critical entities and repealing Council Directive 2008/114/EC, irrespective of their size;

f) Any other entity of a type listed in Annexes I or II to this Decree-Law, referred to in Article 3(2)(b) to (e), which qualifies as an essential entity based on the respective degree of exposure of the entity to risks, the size of the entity, and the probability of occurrence of incidents and their severity, including their social and economic impact.

2 - For the purposes of this Decree-Law, important entities are entities of the types referred to in Annexes I and II to this Decree-Law that are not considered essential entities under the preceding paragraph.

3 - For the purposes of this Decree-Law, important entities are also entities of one of the types listed in Annexes I or II to this Decree-Law, referred to in Article 3(2)(b) to (e), which

justify such qualification on the basis of the respective degree of exposure of the entity to risks, the size of the entity and the probability of occurrence of incidents and their severity, including their social and economic impact.

4 - The attribution of the qualifications of essential entities and important entities provided for in the preceding paragraphs results from the mechanisms provided for in Article 8.

Article 7

Relevant public entities

1 - Public entities that are not qualified as essential or important entities under the terms of the previous article shall be considered relevant public entities, integrating into two groups for the purposes of applying specific regimes under this Decree-Law and remaining regulations issued by the CNCS.

2 - The following are considered relevant public entities of Group A:

a) Central and peripheral direct state administration services with 250 or more employees in their establishment plan;

b) The services of the direct administration of the Autonomous Regions, central and peripheral, with 250 or more employees in their staff establishment plan;

c) Entities of the indirect administration of the State, with more than 250 employees in their staff establishment plan;

d) Entities of the indirect administration of the Autonomous Regions, with more than 250 employees in their establishment plan;

e) Self-government entities with more than 250 employees in their staff establishment plan:

f) Public business entities that exceed the thresholds provided for in Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May;

g) Independent administrative entities;

h) The Economic and Social Council, the Ombudsman's Office, the technical and administrative services of the Presidency of the Republic, the Assembly of the Republic, the Courts and the secretariats with competence for the processing of procedures, the High Council of the Judiciary, the High Council of Administrative and Tax Courts and the High Council of the Public Prosecution Service.

3 - The following are considered relevant public entities of Group B:

a) Central and peripheral direct State administration departments with between 50 and 249 employees in their staff establishment;

b) The direct administration services of the central and peripheral Autonomous Regions, which have between 50 and 249 employees in their establishment plan;

c) Entities of the indirect administration of the State, which have between 50 and 249 employees in their staff establishment plan;

d) Entities of the indirect administration of the Autonomous Regions, which have between 50 and 249 employees in their establishment plan;

e) Self-government entities with between 50 and 249 employees in their staff establishment plan;

f) Public business entities qualified as medium-sized enterprises in accordance with Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May.

4 - The attribution of the envisaged qualification as a relevant public entity **in the preceding paragraphs** results from the qualification mechanisms provided for in the following article.

Article 8

Entity qualification procedure

1 - The entities referred to in Article 3 of this Decree-Law shall identify themselves on an electronic platform provided by the CNCS, within 30 days of the start of their activity or, if the entity is already active at the time of the entry into force of this Decree-Law, within 60 days after the availability of the said electronic platform, being responsible for keeping this

information duly updated.

2 - The classification of entities by the CNCS on the basis of the criteria laid down in Article 6(1)(a) to (c) and (e) and (2), and also in Article 7, is the result of the mechanism provided for in the preceding paragraph.

3 - The qualification of entities by the CNCS on the basis of the criteria set out in Article 6(1)(d) and (f) and (3) shall be notified at least 60 days in advance to the member of the Government responsible for cybersecurity and reviewed at least every two years.

4 - The qualification provided for in the preceding paragraph shall be duly substantiated by the CNCS and shall be preceded by a prior hearing of the entity concerned and, where applicable, by an opinion of the sectoral national cybersecurity authorities referred to in Article 15(2)(a).

5 - The CNCS, or, where applicable, the national sectoral cybersecurity authorities competent in accordance with Article 15(2)(a), shall notify the entity of their qualification in accordance with paragraphs 2 and 3 of this Article within a maximum of 30 days from the date of that qualification.

6 - Providers of domain name registration services shall identify themselves and communicate the information referred to in Article **35**(2) through the electronic platform provided by the CNCS, within 30 days after the start of their activity.

7 - The rules for the operation of the electronic platform referred to in this Article shall be laid down in a regulation to be adopted by the CNCS.

8 - The qualification procedure referred to in this Article shall be without prejudice, for the entities concerned, to the fulfilment of the obligation laid down in Article 35.

Article 9

Competition for qualifications and cybersecurity measures

1 - Where an entity qualifies simultaneously for more than one qualification, the most demanding regime shall be applied to manage the risks posed to the security of network and information systems, in the following order:

a) Essential entities;

b) Important entities;

c) Relevant public entities of Group A;

d) Relevant public entities of Group B.

2 - The CNCS may associate with the qualification of the entity, in accordance with paragraph 4 of Article 26 and Article 33, cybersecurity measures and other technical and organisational measures resulting from the instruments provided for in this Decree-Law, non-compliance with which may determine the application of the corresponding penalties in accordance with the penalty regime provided for in Chapter VII of this Decree-Law.

Article 10

Draft Law No .....

Handling of personal data

1 - The entities that are part of the institutional framework for cyberspace security, pursuant to Article 15, process personal data to the extent strictly necessary to ensure compliance with legal obligations and the pursuit of missions of public interest or public authority in which they are invested, in accordance with the provisions of Article 6(1)(c) or (e) and (3) of the GDPR and in accordance with this Decree-Law and other applicable national legislation.

2 - Entities forming part of the cyberspace security institutional framework may also process personal data for the pursuit of a legitimate interest of essential and important entities, as referred to in Article 6(1)(f) of the GDPR.

3 - Without prejudice to Article 29 of Law No 58/2019 of 8 August, entities forming part of the institutional framework for cyberspace security may process special categories of personal data to the extent strictly necessary:

a) Prevent the occurrence of a significant cyber threat to the security of network and information systems;

b) Respond effectively to a cybersecurity incident.

Chapter Two

Structuring instruments

Draft Law No .....

Article 11

Structuring Instruments of Cyberspace Security

They are structuring instruments of Cyberspace Security, observing the applicable national and international legal and regulatory provisions:

a) National Cybersecurity Strategy;

b) National response plan for large-scale cybersecurity incidents and crises;

c) National Cybersecurity Reference Framework (QNRCS);

d) National Cyber Defence Strategy;

e) Strategic Concept of National Defence.

Article 12

National Cybersecurity Strategy

1 - The National Cyberspace Security Strategy (ENSC) defines the framework, priorities, national strategic objectives and a governance framework defining the roles and responsibilities of stakeholders at national level relevant to the implementation of the ENSC.

2 - ENCS includes, *inter alia*:

a) The objectives and priorities of the ENCS, covering, in particular, the sectors in Annexes I and II to this Decree-Law;

b) A governance framework to meet the objectives and priorities referred to in point (a) of this paragraph;

c) A governance framework defining the roles and responsibilities of stakeholders at national level relevant to the implementation of the ENSC and consolidating institutional cooperation and coordination under this Decree-Law;

d) A mechanism to identify relevant assets and a risk assessment in Portugal;

e) Identification of preparedness, response, and recovery measures in case of incidents, including public-private cooperation;

f) A list of the various authorities and stakeholders involved in the implementation of the ENCS;

g) A policy framework for enhanced cooperation between competent authorities pursuant to this Decree-Law and competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December for the purposes of information sharing on risks, cyber threats and incidents, as well as non-cyber risks, threats and incidents, and the exercise of supervisory tasks;

h) A plan, including the necessary measures, to enhance the general level of education, training and awareness of citizens on cybersecurity and cyber hygiene;

Draft Law No .....

i) A plan, including the necessary measures, appropriate to the specific cybersecurity needs of small and medium-sized enterprises, qualified in accordance with Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May;

j) Promoting the development, research and integration of advanced technologies for the implementation of innovative measures, best practices and controls, including the use of artificial intelligence, in cybersecurity risk management and in the detection and prevention of cyber-attacks.

3 - The ENSC is approved by resolution of the Council of Ministers, on a proposal from the National Cybersecurity Centre (CNCS), after hearing the Superior Council for Cyberspace Security (CSSC), after a period of public consultation of no less than 30 days.

4 - The ENCS is reviewed and updated every five years, following an evaluation process based on key impact and performance indicators, and this period may be reduced by decision of the member of the Government responsible for cybersecurity upon a reasoned proposal from the CNCS.

5 - The ENSC shall be without prejudice to the approval by the competent authorities, where necessary, of instruments establishing sectoral cybersecurity strategies, which shall be reviewed and updated in the same terms as those applicable to the ENSC.

Draft Law No .....

Article 13

National Plan for Responding to Large-Scale Cybersecurity Crises and Incidents

1 - The National Plan for Response to Large-Scale Cybersecurity Incidents and Crises sets out the objectives and modalities for the management of such large-scale cybersecurity incidents and crises.

2 - The national plan for responding to large-scale cybersecurity crises and incidents shall be approved by a resolution of the Council of Ministers, on a joint proposal from the Secretary-General of the Internal Security System, the Criminal Police, the Security Intelligence Service, the Strategic Defence Information Service, the Cyber Defence Operations Command and the CNCS, the latter being responsible for its implementation, follow-up and monitoring, in close cooperation with the entities making up the crisis office provided for in Article 16(4) of Law 53/2008 of 29 August, as amended by this Decree-Law, and after consulting the CSSC.

3 - The national large-scale cybersecurity incident and crisis response plan shall ensure consistency with existing general crisis management frameworks at national level.

Article 14

National Cybersecurity Reference Framework

1 - The National Cybersecurity Reference Framework

(QNRCS) is the national reference tool for the identification of existing norms, standards and good practices in cybersecurity and information security management.

2 - The QNRCS shall be approved by CNCS regulation, after consulting the CSSC, and shall be updated regularly, at least every five years.

3 - Essential and important entities shall take the QNRCS into account when adopting cybersecurity measures pursuant to Articles 27 et seq.

4 - The sectoral national cybersecurity authorities referred to in point (a) of Article **15**(2) may adopt rules supplementing the QNRCS, by means of their own regulations, in conjunction with the CNCS.

5 - Without prejudice to the previous paragraphs, the application of the QNRCS by the essential, important and relevant public entities shall be the subject of a regulation to be approved by the CNCS, providing for specific cybersecurity measures and levels of compliance.

Chapter III

Institutional framework for cyberspace security

Article 15

Organisation

Draft Law No .....

1 - The institutional framework for cyberspace security shall be composed of the following entities:

a) The CSSC, in its capacity as an advisory body to the Prime Minister in the field of cybersecurity;

b) The CNCS, in its capacity as:

i) National Cybersecurity Authority;

ii) Single point of contact for the purposes of cooperation within the European Union and at the international level, without prejudice to the competences conferred on other entities in the field of international cooperation;

iii) National Cybersecurity Certification Authority;

iv) Member of the National Cybersecurity Incident Response Team.

c) The Secretary-General of the Internal Security System, in his capacity as the national authority for managing large-scale cybersecurity incidents and crises.

2 - They are also part of the institutional framework for cybersecurity:

a) As sectoral national cybersecurity authorities:

i) the National Security Office (NSO) with regard to trust services in electronic transactions in the internal market;

ii) The National Communications Authority (ANACOM),

with regard to electronic communications and the postal service.

b) As special national cybersecurity authorities, with regard to the matter of digital operational resilience of the financial sector:

i) The Supervisory Authority for Insurance and Pension Funds (ASF);

ii) The Securities Market Commission (CMVM);

iii) The Bank of Portugal.

c) The Cyberspace Security Assessment Commission;

d) The Judicial Police;

e) The Security Intelligence Service;

f) The Strategic Defence Intelligence Service;

g) The Cyber Defence Operations Command.

3 - The organisation of the institutional framework for cyberspace security shall be without prejudice to the informal coordination of the authorities referred to in this Article, including through participation in multilateral coordination fora concerning the defence of cyberspace security, such as the Cyberspace Liaison Officers Office for tactical-operational cooperation (G5).

Article 16

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Supreme Council for Cyberspace Security

1 - The CSSC is the strategic coordination body supporting the Prime Minister on cybersecurity.

2 - The CSSC is composed of:

a) the Prime Minister, who presides, or the member of the Government responsible for cybersecurity with delegated competence;

b) Two Members appointed by the Assembly of the Republic using the d'Hondt method;

c) The Secretary-General of the Internal Security System;

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

e) The Director of the Security Intelligence Service;

f) The Director of the Strategic Defence Intelligence Service;

g) The Director-General of the National Security Office;

h) The CNCS Coordinator;

i) The Ambassador for Cyber Diplomacy;

j) The Head of the Communications and Information Centre, Cyberspace and Space of the Armed Forces General Staff;

k) The Director of the National Unit for Combating Cybercrime and Technological Crime of the Criminal Police;

l) A representative of the Public Prosecution Service, appointed by the Attorney General of the Republic;

m) The President of the National Council for Emergency Civil Planning;

n) A representative of the National Network of Computer Security Incident Response Teams;

o) The top leader of the sectoral and special national cybersecurity authorities referred to in Article 15(2), not listed in the previous sub-paragraphs.

3 - The CSSC is also composed of a representative of the Regional Government of the Azores and a representative of the Regional Government of Madeira.

4 - The Chair, on his or her own initiative or at the request of any of the members of the CSSC, may convene other holders of public office or invite other entities and persons of recognised merit to attend meetings.

5 - The President shall be replaced in his absence and incapacity by the member of the **G**overnment he designates.

Article 17

Powers of the High Council of Cybersecurity

1 - The CSSC's responsibilities are:

a) Ensure strategic coordination for the security of cyberspace;

b) Issue a prior opinion on the ENSC, monitor its implementation, and draw up an annual or, where necessary, evaluation report on it;

c) Issue a prior opinion on the national crisis and incident response plan for large-scale **cybersecurity**;

d) Issue an opinion on matters related to the security of Cyberspace, at the request of the Prime Minister, or the member of the Government to whom the Prime Minister delegates, within the scope of their competences;

e) Respond to requests from the Prime Minister, or the member of the Government to whom the Prime Minister delegates, within the scope of their powers;

f) Propose to the member of the Government responsible for cybersecurity to carry out security assessments, in accordance with the provisions of the following article.

2 - The annual report evaluating the implementation of the National Cyberspace Security Strategy shall be sent to the Assembly of the Republic by 30 June of the year following that to which it relates.

3 - The Intelligence Services instruct the Supreme Cyber Security Council on the assessment of the current threat to the national cyberspace and the international cyberspace, whenever it is convenient or the threat level assigned by the Intelligence Service is reviewed.

Article 18.

Cyberspace Security Assessment Commission

1 - The Cyberspace Security Assessment Committee

operates alongside the CSSC and is responsible for conducting security assessments of information and communication technology equipment, components or services used in public or private networks and information systems, from manufacturers or suppliers that may be considered high-risk to the security of cyberspace of national interest, namely in the contexts of internal and external security, national defence, the integrity of the democratic process and other sovereign functions, as well as the operation of critical infrastructure and the provision of essential services.

2 - The Cyberspace Security Assessment Commission has the following composition:

a) The Director-General of the National Security Office, who presides;

b) The CNCS coordinator;

c) A representative of ANACOM;

d) A representative of the Internal Security System;

e) A representative of the Information System of the Portuguese Republic;

f) The Ambassador for Cyber Diplomacy;

g) A representative of the Judicial Police;

h) A representative of the Security Intelligence Service;

i) A representative of the Strategic Defence Intelligence Service;

Draft Law No .....

j) A representative of the Cyber Defence Operations Command;

k) A representative of the Directorate-General for External Policy;

l) A representative of the Directorate-General for Defence Policy;

m) A representative of the Competition Authority.

3 - The member of the Government responsible for cybersecurity may determine the application of provisional restrictions on the use, cessation of use or exclusion of information and communication technology equipment, components or services used in public or private networks and information systems, considered to be of high risk to the security of cyberspace of national interest, upon a proposal from the Cyberspace Security Assessment Commission carried out in accordance with the provisions of the following paragraphs.

4 - The evaluation of security must be duly substantiated, taking into account the technical risks of equipment, components or services, their context of use, and the exposure of their manufacturers or suppliers to undue influence from foreign countries, considering, in particular, relevant information issued by national competent authorities and the European Union or contained in national or European risk assessments for the security of network and information systems, as well as other relevant security risks.

Draft Law No .....

5 - To assess the level of exposure of manufacturers or suppliers to undue influence from a foreign country, the following elements may be considered:

a) The manufacturer or supplier is subject, directly or indirectly, to interference by the government or administration of a foreign country;

b) The manufacturer or supplier is domiciled in, or otherwise relevantly linked to, countries recognised by Portugal, the European Union, the Organisation for Economic Co-operation and Development or the North Atlantic Treaty Organisation as responsible for or involved in actions hostile to the internal security and national defence of Portugal or its allies, including acts of espionage or sabotage;

c) The manufacturer or supplier is domiciled in, or in any way relevantly linked to, countries that do not have legislation or diplomatic agreements with Portugal or the European Union on data protection, cybersecurity and intellectual property protection.

d) The manufacturer or supplier is associated with practices of introducing vulnerabilities or hidden access;

e) The manufacturer or supplier adopts corporate governance models that do not clarify the degree of influence or attachment to foreign countries under the conditions of the preceding points;

f) The manufacturer’s or supplier’s production and supply

chains show systemic control and safety failures.

6 - Security assessments may be carried out or reviewed at the request of the member of the Government responsible for cybersecurity, as well as, in application of the Portuguese mechanism for safeguarding key strategic assets, at the request of the member of the Government responsible for the area in which the strategic asset in question is integrated,

7 - The Commission may request any entity, public or private, to provide any information necessary for the preparation of security assessments.

8 - The decision of the member of the **G**overnment responsible for the area of cybersecurity referred to in paragraph 3 shall define the reasonable timeframes and, where applicable, the geographical scope of the measure to be applied, so that the public or private entities concerned implement it.

9 - Documents or information produced in the course of the Commission's work are considered as information classified at the security level Reserved, unless the President of the Commission considers it necessary to assign a higher security classification level, and without prejudice to these documents or information being classified as State secrets pursuant to Organic Law No 2/2014 of 6 August, as amended.

10 - In the exercise of its powers, the CNCS or, where applicable, the national sectoral or special national authority, shall monitor compliance with the requests of the Commission

and the decision of the member of the **G**overnment responsible for the area of cybersecurity provided for in this Article, sanctioning its non-compliance in accordance with Article 63(1)(d) and Article 61(1)(a), respectively.

11 - The technical, administrative and logistical support of the Commission, as well as the associated costs, shall be provided and borne by the GNS.

Article 19

National Cybersecurity Centre

1 - The National Cybersecurity Centre (CNCS) is the national cybersecurity authority, whose mission is to ensure that the country achieves and maintains a high level of cybersecurity, through the promotion of continuous improvement of national cybersecurity and international cooperation, as well as the definition and implementation of the measures and instruments necessary for the anticipation, detection, reaction and recovery of situations that, in the face of the imminence or occurrence of incidents, jeopardise the national interest, the functioning of essential entities, important entities and relevant public entities.

2 - The CNCS is also the single point of contact for the purposes of cooperation at the European Union level, as well as at the international level on cybersecurity, without prejudice to the powers conferred on other authorities with regard to cooperation in criminal matters, in particular the powers of the Criminal

Draft Law No .....

Police for international cooperation conferred on it by Articles 20 to 26 and Article 29 of the Cybercrime Law, and with regard to the production of information relating to the internal and external security of the Portuguese State and its allies.

3 - The CNCS is part of the 'CERT.PT', provided for in Article 22, which acts as the National Cybersecurity Incident Response Team.

4 - The CNCS is also the national cybersecurity certification authority, in particular for the purposes of Article 58 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April, without prejudice to the competences of the GNS as regards the certification and accreditation of information and communication systems processing classified information, pursuant to Decree-Law No 3/2012 of 16 January, as amended.

Article 20.

Competences of CNCS

1 - The CNCS, within the scope of the responsibilities assigned in Article 19(1) and (2), shall perform the tasks and exercise the powers described in the following points;

a) Develop national capacities for prevention, monitoring, detection, reaction, analysis, and correction to address cybersecurity incidents, cyber-attacks and cyber-threats;

b) Cooperate with the competent entities in the field of cyberspace security within the scope of their respective

responsibilities;

c) Communicate, within 24 hours, to the Judicial Police all facts with criminal relevance of which it becomes aware in the course of its activity;
d) Report within 24 hours to the Security Intelligence Service all facts concerning threats to internal security, cyber-espionage, and cyber-sabotage of which it becomes aware in the course of its activity;
e) Adopt regulations and issue guidelines, recommendations and technical instructions relating to cybersecurity;
f) Propose to the member of the Government responsible for cybersecurity the definition of the national level of cybersecurity alert, developed through the CNCS's own regulation and disseminated in coordination with the competent entities in the field of cyberspace security, and issue orders and instructions appropriate to the seriousness of the situation;
g) Inform the Secretary-General of the Internal Security System about the verification of a significant cyber threat or the occurrence of a large-scale cybersecurity crisis or incident pursuant to Article 2(d) and (k) respectively and without prejudice to Article 21(2);
h) Issue orders, guidelines, recommendations and technical instructions on coordinated vulnerability disclosure;
i) Prevent and mitigate the impact of cybersecurity incidents, including by detecting and disclosing vulnerabilities in network and information systems, in collaboration with

public and private entities, natural and legal persons;

j) Apply supervisory and enforcement measures in accordance with Chapter VI;

k) Issue warnings, including on vulnerabilities, concerning malware or other cybersecurity risks in ICT products, components or services;

l) Ensure cross-border cooperation with the competent authorities of the Member States of the European Union, with the European Commission, the European Union Agency for Cybersecurity (ENISA) and other European Union institutions, bodies and agencies active in the field of cybersecurity and the competences conferred upon it by this Article, including participation and national representation in multilateral and bilateral fora with their counterparts, without prejudice to Articles 20 to 26 and 29 of the Cybercrime Act, including national participation and representation:

i) the Cooperation Group provided for in Article 14 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December;

ii) In the European Network of CSIRTs (Computer Security Incident Response Team), as provided for in Article 15 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December; and

iii) the Cyber Crisis Liaison Organisation Network (EU-CyCLONe) provided for in Article 16 of Directive (EU)

Draft Law No .....

2022/2555 of the European Parliament and of the Council of 14 December.

m) Issue a non-binding opinion, when requested, on any legislative measure relating to cybersecurity;
n) Promote awareness, training, and qualification of human resources in the area of cybersecurity, with a view to forming a knowledge community and a national cybersecurity and cyber-hygiene culture;
o) Support the development of technical, scientific and industrial capacities by promoting innovation and development projects in the area of cybersecurity;
p) Publish studies and reports in the area of cybersecurity;
q) Approve the forms necessary for the performance of its tasks.

2 - The CNCS shall, in the exercise of the responsibilities assigned by Article 19(4), carry out the tasks and exercise the powers described in the following points:

a) Request from conformity assessment bodies, holders of cybersecurity certificates, and issuers of statements of conformity the information necessary for the exercise of their powers;

b) Take appropriate measures to ensure that conformity assessment bodies, holders of national or European cybersecurity certificates, and issuers of statements of conformity comply with the applicable legislation on cybersecurity certification;

c) Exercise the other powers legally established for cybersecurity certification authorities, in particular those resulting from Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April, without prejudice to the powers of the GNS as regards the certification and accreditation of information and communication systems processing classified information, pursuant to Decree-Law No 3/2012 of 16 January, as amended;

d) Implement a national cybersecurity certification framework, laying down the necessary provisions for the preparation, implementation and enforcement of certification regimes, to which the provisions of Title III of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April shall apply *mutatis mutandis*;

e) Evaluate the specific certification regimes, in particular their adequacy, liaising with the Portuguese Accreditation Institute (Instituto Português de Acreditação, I.P.), as the national accreditation body, as well as with the Portuguese Quality Institute (Instituto Português da Qualidade, I.P.), as the national standardisation body, and with other public entities with competence in the field covered by the certification;

f) Develop and implement specific cybersecurity certification regimes for information and communication technology entities, products, services, and processes that are not yet

covered by a European regime, where justified by the specificity of the subject matter of the certification;

g) Promote the training of auditors in the field of cybersecurity, in collaboration with the Portuguese Accreditation Institute, I.P.

3 - Any cybersecurity regulatory provision issued by national sectoral or special cybersecurity authorities shall be preceded by an opinion of the CNCS.

4 - As public and private entities shall cooperate with the CNCS in the exercise of their respective powers and responsibilities under this Decree-Law, in accordance with the principle of proportionality.

5 - The duty of cooperation provided for in the preceding paragraph may include physical access to the premises of entities to carry out due diligence integrated in supervisory or incident response actions, without prejudice to compliance with access requirements provided for in other special information security regimes and in compliance with the requirements laid down in the Code of Administrative Procedure.

6 - The CNCS acts in close cooperation with the national structures responsible for cyber espionage, cyber defence, cybercrime and cyberterrorism.

Article 21

Draft Law No .....

Cybersecurity Crisis Management Authority

1 - The Secretary-General of the Internal Security System is the national authority for managing large-scale cybersecurity incidents and crises, also referred to as the cybersecurity crisis management authority.

2 - The declaration of large-scale cybersecurity incidents and crises depends on the attribution of a 'high' threat level by the Security Intelligence Service, in accordance with the Plan for the coordination, control and operational command of the Security Forces and Services, approved by Council of Ministers Decision No DB 14/2010 of 5 March, or on the communication by the CNCS of the occurrence of a large-scale cybersecurity incident or crisis, in accordance with Article 20(1)(g).

3 - The Secretary-General of the Internal Security System shall convene the Cybersecurity Crisis Office, pursuant to Article 16(4) of Law No 53/2008 of 29 August, as amended,

Article 22

Cybersecurity Incident Response Team

1 - 'CERT.PT' is the national cybersecurity incident response team.

2 - 'CERT.PT' is integrated into the CNCS and has technical and operational autonomy.

3 - 'CERT.PT' shall exercise the following competences:

a) Ensure operational incident response;

b) Monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, assisting relevant essential, important and public entities with real-time or near-real-time monitoring of their networked systems and information;

c) Activate early warning mechanisms, send alert messages, communicate and disseminate information to relevant essential, important and public entities, competent authorities, and other stakeholders, on cyber threats, vulnerabilities and incidents, including in real time;

d) Intervene in the event of incidents and provide assistance to relevant essential, important, and public entities, including, where applicable, by proposing to the CNCS the issuance of operational orders, instructions, and guidelines on measures to be taken to contain, mitigate, and resolve incidents, as well as appropriate deadlines for their implementation;

e) In situations of proven serious risk, propose to the competent cybersecurity authority the adoption of implementing measures necessary for an immediate response to the cyber threat, incident or crisis, in accordance with Article 52(3), where the relevant essential, important or public entity concerned does not do so on a voluntary basis;

f) Collect and analyse forensic data, determine its

preservation, perform dynamic risk and incident analysis, and develop cybersecurity situational awareness;

g) Carry out, at the request of a relevant essential, important or public entity, a proactive analysis of the entity's respective network and information systems in order to detect vulnerabilities with a potential significant impact;

h) Implement tools and functionalities that enable the secure sharing of information with essential, important, and relevant public entities, as well as with other stakeholders;

i) Carry out, on its own initiative, proactive and non-intrusive analyses of publicly accessible network and information systems of relevant essential, important and public entities, with the aim of detecting vulnerable or unsafe network and information systems and informing the entities concerned, insofar as they do not have any negative impact on the functioning of their services;

j) Promote the adoption and use of common or standardised practices;

k) Ensure national representation in the network of national cybersecurity incident response teams pursuant to Article 20(1)(l)(ii) and other international forums for cooperation of cybersecurity incident response teams;

l) Participate in national forums for cooperation of

Computer Security Incident Response Teams;

m) Participate in national and international events and training sessions;

n) Collaborate and coordinate with sectoral, national, and European CSIRTs networks, whenever necessary or appropriate;

o) Cooperate with the competent entities in the field of cyberspace security.

4 - In the exercise of its powers, 'CERT.PT' may determine the prioritisation of certain tasks through a risk-based approach, taking into account, *inter alia*, the existing threat assessment produced by the Security Intelligence Service.

5 - Public and private entities shall cooperate with 'CERT.PT' in the exercise of their respective tasks and powers under this Decree-Law.

6 - The collaboration referred to in the previous paragraph may include physical access to facilities and information sharing between entities providing incident response services to third parties and 'CERT.PT', and joint actions, at its initiative, for the purposes of (3)(e).

Article 23

Cooperation between national authorities

1 - The CNCS, the Secretary-General of the Internal Security System, and the national sectoral cybersecurity authorities,

in the exercise of their tasks and powers under this Decree-Law, shall act in close cooperation with:

a) The National Data Protection Commission, whenever incidents giving rise to a personal data breach are concerned, in accordance with Article 79;

b) The Public Prosecutor's Office, the courts, and the Judicial Police, whenever incidents are involved that may have led to the commission of cybercrimes, namely through:

   i) The communication, as soon as possible, of facts relating to the preparation and execution of cybercrimes of which they have become aware in the exercise of their functions, without prejudice to the provisions of Article 38 of this Decree-Law;

   ii) The practice of the necessary and urgent precautionary acts to ensure the preservation of evidence and the sharing, in legal terms, of other evidence necessary for the strict exercise of the powers provided for in (3)(a) to (e) of the preceding Article;

   iii) the performance of the function of expert provided for in Article 153 of the Code of Criminal Procedure.

c) The Cyber Defence Operations Command, namely when it concerns incident prevention, monitoring, detection,

reaction, analysis, and correction in the context of cyber defence and cyber security of the Armed Forces;

d) The Security Intelligence Service, in particular in the sharing of information necessary for the preservation of the security of cyberspace of national interest, in particular as regards espionage, sabotage, terrorism and organised crime.

2 - Obtaining information under the cooperation provided for in the preceding paragraph must comply with the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August, and Law No 59/2019 of 8 August.

3 - The cooperation provided for in point (b) of paragraph 1 shall not jeopardise the confidentiality of judicial proceedings.

4 - Access to information in accordance with the cooperation provided for, in particular, in (1)(b)(i) and (ii), relating to cases under investigation, may be refused on the grounds provided for in Article 89(1) of the Code of Criminal Procedure.

5 - The Judiciary Police and the Security Intelligence Service shall designate a permanent liaison officer to the CNCS.

6 - The terms of technical and operational cooperation between the CNCS, the Cyber Defence Operations

Command, the Criminal Police, the Security Intelligence Service and the Strategic Defence Intelligence Service are defined by mutual agreement within the G5.

7 - The authorities referred to in this Article shall reply to requests for information within five days of the date on which the information was requested, unless there are duly justified grounds.

Article 24

Cooperation with the private sector

1 - Entities that are part of the institutional framework for cyberspace security, in accordance with Article 15, shall establish cooperative relations with the entities covered by this Decree-Law and, where relevant, with other private sector stakeholders, with a view to achieving the objectives of the cybersecurity legal regime.

2 - Cooperation relations shall cover at least the following aspects relating to the sharing of information, the adoption of best practices, the development or improvement of common or standardised classification systems and taxonomies with regard to:

a) Cybersecurity risk management measures;

b) Indicators of exposure to risks or cyber threats;

c) Incident handling procedures;

d) Crisis management; and

e) Coordinated vulnerability disclosure in accordance with Article 38.

3 - In order to promote the exchange of knowledge, the sharing of best practices and the mobilisation of expertise from private sector entities in support of the relevant cybersecurity authority, public-private partnerships for cybersecurity may be adopted, defining the scope and the parties involved, the governance model, the available funding options and the interaction between the participating parties.

4 - Cybersecurity information sharing agreements may be concluded between the entities referred to in paragraph 1 as well as, where relevant, with their suppliers or service providers, for the following purposes:

a) Preventing, detecting, responding to, and recovering from incidents or mitigating their impact;

b) Enhancing the level of cybersecurity, in particular by raising awareness of cyber threats, limiting or impeding their dissemination capacity, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies or response and recovery phases, or promoting collaborative investigation of cyber threats between public and private entities.

5 - The parties to the information-sharing agreements shall,

where necessary, take measures to protect the sensitive nature of the information shared and limit its distribution, in accordance with the so-called TLP (Traffic Light Protocol).

6 - Essential and important entities are required to notify the competent cybersecurity authority of their participation in the agreements referred to in paragraph 4 at the time of their conclusion or, where applicable, of their withdrawal from such agreements, as soon as it becomes effective.

7 - The agreements referred to in paragraph 4, when concluded by essential and important entities covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December on digital operational resilience for the financial sector, shall be communicated to their respective special national cybersecurity authorities.

8 - The CNCS ensures and manages an online platform for information sharing.

Chapter IV

Cybersecurity risk management and other duties

Section I

Cybersecurity and Information Security Management

Draft Law No .....

Article 25

Obligations of management, direction and administrative bodies

1 - The management, direction and administrative bodies of essential and important entities shall:

a) Approve the cybersecurity risk-management measures adopted in accordance with Article 27;

b) Oversee the implementation of cybersecurity risk management measures;

c) Ensure compliance with the supervisory and enforcement measures referred to in Chapter VI of this Decree-Law;

d) Ensure the regular conduct of cybersecurity training to promote an internal management culture on cybersecurity risk management practices.

2 - The holders of the management, direction and administrative bodies may be held liable by action or omission, intentionally or with serious fault, in accordance with the applicable legislation, for the infringements provided for in this Decree-Law.

3 - The responsibility and powers necessary for the fulfilment of the obligations referred to in this Article may not be delegated, except to one of the holders of the management, direction and administrative bodies.

Draft Law No .....

Article 26

Cybersecurity risk management system

1 - Essential and important entities shall be responsible for ensuring the security of network and information systems by taking appropriate technical, operational and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations and to prevent or minimise the impact of incidents on recipients of their services and on other services.

2 - Cybersecurity measures adopted shall be based on a systemic approach covering all risks for essential and important entities and aiming at protecting all assets ensuring the continued operation of the network and information systems supporting essential services, including their physical environment, against incidents.

3 - The measures should also:

a) Ensure a level of security of network and information systems appropriate to the risk at stake, taking into account the latest technical developments and, where applicable, relevant European and international standards, as well as their implementation costs and financial viability; and

b) Be proportionate to the extent of the entity's exposure to risks, the size of the entity, and the probability of occurrence of incidents and their severity, including their social and economic impact, in accordance with the

technical criteria to be defined by the CNCS.

4 - In order to guide the cybersecurity risk management policy of essential and important entities, the CNCS may issue technical harmonisation instructions and, where necessary, develop and update the risk matrix applicable to those entities.

5 - Considering the sector of activity, the size of the entity, and the defined risk matrix, the CNCS, through a regulation to be approved by the CNCS, defines minimum and specific cybersecurity measures and levels of compliance to be adopted by essential entities and important entities.

6 - The minimum cybersecurity measures shall be without prejudice to the adoption of other measures that are necessary and proportionate as a result of the analysis and management of residual cybersecurity risks, in accordance with the following Article.

7 - The relevant public entities shall adopt the appropriate technical, operational and organisational measures as determined by the CNCS, in accordance with the group to which they belong, pursuant to Article 33.

Article 27

Cybersecurity measures

1 - The cybersecurity measures to be adopted by essential and important entities, taking into account the risk matrix in which they are inserted in accordance with Article 26, shall

cover, *inter alia,* the following areas:

a) Incident handling;

b) business continuity, such as backup management and disaster recovery, and crisis management;

c) Supply chain security, including security aspects concerning the relationships between each entity and its direct suppliers or service providers;

d) Security in the acquisition, development and maintenance of network and information systems, including vulnerability handling and disclosure;

e) Policies and procedures to assess the effectiveness of cybersecurity risk management measures;

f) Basic cyber hygiene practices and cybersecurity training, including senior management and employees;

g) Policies and procedures relating to the use of cryptography and, where appropriate, encryption, without prejudice to the powers conferred on other entities in the field of cryptography at national level or before other international organisations of which Portugal is a member;

h) Human resources security, access control policies, and asset management;

i) Use of multi-factor authentication or continuous authentication, secure communications, and secure emergency communications systems within the entity.

2 - Essential and important entities shall also adopt, without undue delay, all necessary, appropriate and proportionate corrective cybersecurity measures that are indispensable for remedying failures or omissions in complying with the measures provided for in the preceding paragraph.

3 - Sectoral national cybersecurity authorities may issue regulatory provisions for sector-specific cybersecurity measures, without prejudice to the provisions of Article 20(3).

Article 28

Supply chain

Cybersecurity measures relating to supply chain security, including security aspects relating to the relationships between each entity and its direct suppliers or service providers, shall consider, *inter alia*:

a) The vulnerabilities specific to each direct supplier and service provider;

b) The overall quality of the products in the cybersecurity component;

c) the cybersecurity practices of their suppliers and service providers, including their secure development procedures;

d) the coordinated security risk assessments of supply chains of critical ICT products, ICT systems or ICT services that are carried out pursuant to Article 22 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December;

e) Decisions on the application of restrictions on the use, cessation of use or exclusion of information and communication technology equipment, components or services pursuant to Article 18(3).

Article 29

Residual Risk Management

1 - Essential and important entities shall perform risk analysis and risk management in relation to all assets that ensure the continuity of the operation of the network and information systems they use, including assets that guarantee the provision of essential services, with the periodicity and technical and documentary elements to be defined by regulation of the competent cybersecurity authority, in addition to compliance with minimum cybersecurity measures pursuant to Article 26(4) and (5).

2 - On the basis of the risk analysis and management referred to in the previous paragraph, essential and important entities shall adopt appropriate and proportionate cybersecurity measures in order to manage the risks posed to the security of the network and information systems they use, including residual risks, taking into account the QNRCS, the latest technical developments and, where applicable, relevant European and international standards.

Draft Law No .....

3 - Essential and important entities shall document the preparation, execution, and presentation of the results of the risk analysis.

Article 30

Annual report

1 - Essential and important entities shall draw up and maintain an annual report containing the following elements for the calendar year to which they refer:

a) A summary description of the main activities carried out in the field of network and information services security;

b) Quarterly statistics of all incidents, indicating the number and type of incidents;

c) Aggregated analysis of incidents with significant impact, with information on:

i) Number of users affected by the service disruption;

ii) Duration of incidents;

iii) Geographical distribution concerning the area affected by the incidents, including an indication of cross-border impact.

d) Recommendations for activities, measures or practices that promote the improvement of the security of network and information systems;

e) Problems identified and measures implemented following

the incidents;

f) Any other information deemed relevant.

2 - The essential entities shall submit the annual report to the competent cybersecurity authority, duly signed by the Cybersecurity Officer, as follows:

a) The first annual report shall be submitted:

i) By the last working day of January of the calendar year following the first calendar year of activity, where the activity began in the first half of the year;

ii) By the last working day of January of the second calendar year following the first calendar year of activity, where the activity began in the second half of the year.

b) Subsequent annual reports shall be submitted by the last working day of January of the calendar year following the year to which they relate.

3 - For the purposes of point (a)(ii) of the preceding paragraph, the annual report shall also cover the period between the date of commencement of activity and the end of the calendar year preceding that to which it relates.

4 - Important entities shall communicate the annual report to the CNCS whenever requested.

5 - The CNCS, after consulting the national sectoral cybersecurity authorities, may adopt templates for the submission of the report referred to in the preceding

paragraphs.

Article 31

Cybersecurity Officer

1 - Essential and important entities shall designate a cybersecurity officer for the management of cybersecurity and information security, who shall be a member of, or report directly and organically to, the management, executive, or administrative bodies.

2 - The Cybersecurity Officer shall have at least the following functions:

a) Propose the cybersecurity risk management measures, including at the level of the supply chain, which must be approved in accordance with Article 25(1)(a);

b) provide information on cybersecurity risk management measures to the bodies of the entity responsible for their supervision as provided for in Article 25(1)(b);

c) assist the bodies of the entity in complying with the supervisory and enforcement measures pursuant to Article 25(1)(c);

d) Contribute to the promotion of a cybersecurity culture within the entity, proposing, in particular, the cybersecurity training actions provided for in Article 25(1)(d);

e) Ensure the risk management provided for in Article 29;

f) ensuring compliance with the obligations relating to the preparation of the annual report pursuant to Article 30;

g) Coordinate the actions of the permanent contact point, as provided for in Article 32, where this function is not ensured by it;

3 - Essential and important entities shall, within 20 working days of taking up their duties, notify the competent cybersecurity authority of the person designated to act as cybersecurity officer, including the information referred to in a regulation to be approved by the CNCS.

4 - Essential and important entities that have commenced activity before the date of entry into force of this Decree-Law are to make the notification provided for in the preceding paragraph within 20 working days from that date.

5 - Essential and important entities shall, without undue delay, communicate to the competent cybersecurity authorities the replacement of the cybersecurity officer.

6 - For essential and important entities belonging to the direct administration, the same Cybersecurity Officer may be designated for several ministries, government areas, or regional secretariats.

7 - For essential and important entities within the same group of undertakings, each undertaking may establish an element to act as a contact point for cybersecurity under the coordination of a common group security officer.

8 - The exercise of the functions of the Cybersecurity Officer shall be compatible with the accumulation of other functions within the same entity, without prejudice to this Article.

Article 32

Permanent contact point

1 - Essential and important entities shall ensure the function of the permanent point of contact with continuous availability 24 hours a day, seven days a week, limited to activation periods, initiated and terminated upon communication from the relevant cybersecurity authority.

2 - Essential and important entities shall report to the CNCS at least one permanent point of contact, which may be provided by a member or a team, in order to ensure:

a) Operational and technical level information flows with the competent cybersecurity authority, namely:

i) Cross-sectoral articulation, including the effectiveness of the response to security incidents with an impact at the sector level;

ii) Obtaining operational and technical information, following notification of incidents with a significant impact submitted by the same or another entity;

iii) Obtaining and updating integrated situational information in the context of a significant incident.

b) Sharing information with the competent cybersecurity authority, when civil protection emergency plans directly related to or impacting cybersecurity are activated, as well as plans under civil cybersecurity emergency planning, national or European critical infrastructure security plans, or the resilience plans of national or European critical entities;

c) The operationalisation of procedures established as part of a civil protection emergency plan when they have an impact on the operation of network and information systems, or civil cybersecurity emergency planning;

d) The receipt of guidelines, recommendations, technical instructions and orders issued by the competent cybersecurity authority.

3 - Essential and important entities shall indicate to the competent cybersecurity authority, within 20 working days of taking up their duties, the person(s) within the team that will act as a permanent point of contact, as well as their main and alternative means of contact containing the information referred to in a regulation to be approved by the CNCS.

4 - Essential and important entities that have commenced activity before the date of entry into force of this Decree-Law shall make the notification provided for in the preceding paragraph within 20 working days from that date.

5 - Essential and important entities shall immediately notify the competent cybersecurity authority of any change to the

information provided for in paragraph 3.

6 - Essential and important entities shall ensure that the permanent point of contact has primary and alternative means of contact for communication with the competent cybersecurity authority.

Article 33

Cybersecurity measures applicable to relevant public entities

1 - Relevant public entities shall comply with the cybersecurity measures established by the CNCS pursuant to the following paragraph.

2 - The CNCS shall establish, by means of a regulation, the cybersecurity measures that must be complied with by the relevant public entities, taking into account the criteria set out in Article 26(2) and (3) and in terms proportionate and appropriate to the group to which they belong, in accordance with Article 7.

3 - The relevant public entities shall be subject to the supervisory and enforcement measures provided for in Articles 55 and 56 respectively.

Article 34

Cybersecurity certification

1 - The CNCS may require essential, important, and relevant

public entities to obtain national, European, or international certification attesting compliance with the cybersecurity measures of this Decree-Law, namely in accordance with certification regimes drawn up from the Portuguese Normative Document - Technical Specification (DNP TS) 4577-1, Digital Maturity - Digital Seal, and the National Reference Framework for Cybersecurity, ensuring, in any case, an equivalence matrix with existing reference certification regimes.

2 - The CNCS may also require relevant essential, important and public entities, pursuant to Article 24(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, to use ICT products, services and processes, all developed by the entity or provided by third parties, certified under national and European cybersecurity certification regimes adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April.

Section II

Other duties

Article 35

Enrolment Duty

1 - For the purposes of registration, relevant essential, important and public entities have the duty to enter in the

electronic platform referred to in Article 8(7) the elements that allow their complete identification, namely:

a) The name of the entity concerned;

b) Tax number,

c) Up-to-date address and contact details, including e-mail addresses, IP address ranges and telephone numbers;

d) Where applicable, the relevant sector and subsector referred to in Annexes I or II to this Decree-Law, which form an integral part thereof; and

e) Where applicable, a list of the Member States of the European Union in which they provide services falling within the scope of this Decree-Law.

2 - In addition to the data referred to in the previous paragraph, the registration of top-level domain names, as well as entities that are DNS service providers, domain name registration service providers, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, have the duty to register the following elements on the electronic platform referred to in Article 8(7):

a) The address of its principal place of business and other legal establishments in the European Union or, where it is not established in the Union, of its designated

representative;

b) Up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its designated representative;

c) The Member States in which it provides services; and

d) The ranges of IP addresses.

3 - Relevant essential, important, public entities and domain name registries service providers shall notify any change to the data referred to in the preceding paragraphs within 30 working days of the change.

4 - In the case of registering TLD names, as well as entities that are DNS service providers, domain name registration service providers, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, the change to the data referred to in (1) and (2) shall be notified within three months of the change.

Article 36

Domain name registration database

1 - The TLD name registry and the entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data in purpose-built

databases.

2 - The collection and maintenance of the data referred to in the preceding paragraph constitutes a legal obligation under and for the purposes of Article 6(1)(c) of the GDPR.

3 - The database referred to in (1) shall contain the following information:

a) The domain name;

b) The date of registration,

c) The name, contact email address and telephone number of the registration holder;

d) The contact address and the contact telephone number administering the domain name, if different from the registration holder.

4 - The TLD name registry and the entities providing domain services shall adopt policies and procedures, including verification, to ensure that their databases, in accordance with (1), contain accurate and complete information.

5 - The data relating to the registration of domain names and the policies and procedures referred to in the preceding paragraphs must be accessible to the public, when they are not personal data and are not protected under the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August and Law No 59/2019 of 8 August.

Draft Law No .....

Article 37

Access to domain name registration

1 - The registration of top-level domain names and entities providing domain name registration services guarantee access to specific data relating to the registration of domain names to those who submit a lawful and duly substantiated request for access, in accordance with the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, as amended, Law No 58/2019 of 8 August, and Law No 59/2019 of 8 August.

2 - Requests for access referred to in the preceding paragraph shall be granted within 72 hours of receipt thereof.

Chapter V

Incident prevention and treatment

Section I

Vulnerability prevention and monitoring

Article 38

Vulnerabilities in information systems

1 - 'CERT.PT' is the national coordinating entity for the coordinated disclosure of vulnerabilities affecting information and communication technology networks and systems,

products, components and services.

2 - ‘CERT.PT’ shall act as a trusted intermediary, facilitating the interaction between the notifying natural or legal person and the manufacturer or provider of potentially vulnerable ICT products or ICT services, at the request of either party.

3 - The tasks of ‘CERT.PT’ shall include, in particular:

a) The identification and contact details of the entities referred to in the preceding paragraph;

b) Providing support to natural or legal persons reporting vulnerabilities;

c) Negotiating the disclosure schedule and managing vulnerabilities affecting multiple entities.

4 - ‘CERT.PT’ shall preserve the anonymity of any natural or legal person who reports a vulnerability if so requested, without prejudice to the provisions of the Cybercrime Law, approved by Law No 109/2009 of 15 September, as amended by this Decree-Law.

5 - The data included in the communications made under this Article shall be deleted within 10 days from the moment the vulnerability is rectified, and their confidentiality shall be guaranteed throughout the procedure.

Article 39

Vulnerability reporting

Draft Law No .....

Where vulnerability may have a major impact on entities in more than one Member State of the European Union, 'CERT.PT' cooperates with its counterparts, either within the European Network of CSIRTs or within the EU-CyCLONe framework.

Section II

Incident notification

Article 40

Mandatory notification

1 - Essential, important, and relevant public entities shall notify any significant incident to the competent cybersecurity authority.

2 - Compliance with the mere notification does not give rise to increased liability on the part of the notifying entity.

3 - In determining whether an incident has a significant impact pursuant to paragraph 1, the entities concerned shall take into account, *inter alia*, the following parameters:

a) Number of users affected by the service disruption;

b) The duration of the incident;

c) The level of severity of the disruption to the operation of the service;

d) The extent of the impact on economic and social activities.

4 - Entities should also take into consideration the parameters and thresholds defined by technical instruction of the CNCS and by the Commission implementing acts, provided for in Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December.

5 - Compliance with the provisions of this Decree-Law shall not exempt compliance with specific incident notification obligations as defined by the competent authorities, namely the Public Prosecutor’s Office, the Judicial Police, the National Data Protection Commission (CNPD), the State Secret Supervisory Authority and the GNS, in accordance with the applicable legal and regulatory provisions.

6 - Notifications shall be submitted on the electronic platform referred to in Article 8(7).

7 - Relevant essential, important and public entities shall be ensured the possibility to notify an incident simultaneously to the competent cybersecurity authority, to the special cybersecurity authorities, as well as to the entities referred to in paragraph 5 of this Article, through the platform provided for in Article 8(7), in accordance with a protocol to be established between those authorities.

Article 41

Draft Law No .....

Types of notifications

1 - For each incident subject to mandatory notification, relevant essential, important, and public entities shall submit:

a) An initial notification in accordance with Article 42;

b) A notification of the end of the significant impact pursuant to Article 43;

c) A final report in accordance with Article 44.

2 - In cases where the incident is resolved within two hours of its detection, the entities referred to are only required to send the notification of the end of significant impact.

3 - Without prejudice to the provisions of the preceding paragraph, relevant essential, important and public entities may still be notified to submit an interim report, pursuant to Article 44.

4 - The incident notification format and procedure and the taxonomy of incidents, including the categories of causes of incidents and their effects, shall be defined by technical instruction of the CNCS, without prejudice to the implementing acts adopted by the Commission provided for in Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December.

Article 42

Initial notification

Draft Law No .....

1 - The initial notification shall be sent to the relevant cybersecurity authority as soon as the relevant essential, important or public entity concludes that a significant incident exists or is likely to occur, without undue delay and no later than **24** hours after that verification, unless this is incompatible with mitigating or resolving the incident.

2 - The initial notification shall include at least the following information:

a) The name, telephone number and email address of a representative of the entity, where different from the permanent point of contact referred to in Article 32, for the purpose of any contact by the competent cybersecurity authority;

b) The date and time of the start or, if this cannot be determined, of the detection of the incident;

c) A brief description of the incident, including an indication of the category of cause and effects produced, according to the taxonomy defined by the CNCS, where possible, the respective detail;

d) Possible estimation of the impact, considering:

i) Number of users affected by the service disruption;

ii) Duration of the incident;

iii) Geographical distribution, as regards the area affected by the incident, including an indication of the cross-border impact;

iv) Other information that the essential and important entity considers relevant.

3 - Where necessary, the relevant essential, important or public entity shall send to the competent cybersecurity authority an update of the initial notification no later than 72 hours after the verification of the significant incident, reviewing the information referred to in the previous paragraph and providing an initial assessment of the significant incident, including its severity and impact, as well as, where available, indicators of exposure to risks.

Article 43

Notification of the end of significant impact

1 - The notification of the end of the significant impact of the incident shall be submitted to the competent cybersecurity authority, without undue delay and within 24 hours of the end of the impact.

2 - The notification of the end of significant impact shall include at least the following information:

a) Updating the information transmitted in the initial notification, if any;

b) A brief description of the measures taken to resolve the incident;

c) Description of the impact situation existing at the time of the loss of significant impact, including:

i) Number of users affected by the service disruption;

ii) Duration of the incident;

iii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact;

iv) Estimated time for full recovery of services.

Article 44

Final and interim reports

1 - The final report shall be submitted to the competent cybersecurity authority within 30 working days from the date of notification of the end of the significant impact of the incident.

2 - The final report shall include the following information:

a) The date and time when the incident assumed the significant impact;

b) The date and time when the incident lost its significant impact;

c) Impact of the incident, considering:

i) Number of users affected by the service disruption;

ii) Duration of the incident;

iii) Geographical distribution, as regards the area affected by the incident, including indication of

cross-border impact;

iv) Description of the incident, indicating the category of cause and effects produced, according to the taxonomy defined by the CNCS, and the respective details;

d) An indication of the measures taken to mitigate the incident;

e) Description of the residual impact situation existing at the time of the final notification, in particular:

i) Number of users affected by the service disruption;

ii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact;

iii) Estimated time for full recovery of services still affected;

iv) Indication, where applicable, of the submission of notification of the incident in question to the competent authorities, namely the Public Prosecutor's Office or the CNPD and other sectoral authorities, in accordance with the applicable laws and regulations;

v) Other information that the essential and important entity considers relevant.

3 - In the event that, after the deadline for submission of the final report, the incident is still ongoing, the relevant

essential, important or public entity concerned shall submit an interim report to the competent cybersecurity authority, at the request of those entities and on a weekly basis until the time the final report is submitted.

4 - The interim report shall include the following information:

a) Updating the information transmitted in the initial notification, if any;

b) A brief description of the measures taken to resolve the incident;

c) Description of the impact situation existing at the time of the loss of significant impact, including:

i) Number of users affected by the service disruption;

ii) Duration of the incident;

iii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact;

iv) Estimated time for full recovery of services.

Article 45.

Voluntary notifications of relevant information

1 - Without prejudice to the incident notification obligation provided for in this Decree-Law, any natural or legal person may notify, on a voluntary basis, the occurrence of incidents,

cyber threats, near misses or vulnerabilities.

2 - Voluntary notifications do not create additional obligations for the notifying entity.

3 - Articles 42 to 44 shall apply *mutatis mutandis* to voluntary notifications, without prejudice to the priority to be given to the processing of mandatory notifications.

Article 46

Enquiries

The competent cybersecurity authority may request relevant information from the relevant essential, important or public entities or determine the necessary actions, in accordance with the law, when it becomes aware, by any means, of a potential incident and Articles 42 to 44 shall apply *mutatis mutandis*.

Article 47

Information protection

1 - The sending of information by the CNCS or, where applicable, by the national sectoral cybersecurity authorities, under this Decree-Law, to competent national authorities or entities of the European Union or of another Member State is limited to what is necessary and proportionate, in accordance with the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, in its

current wording, Law No 58/2019 of 8 August, and Law No 59/2019 of 8 August.

2 - The competent cybersecurity authority shall ensure the adequate protection of information and data, of whatever nature, transmitted by essential, important and public entities relevant to confidentiality and trade secrets.

3 - Paragraph 2 shall apply *mutatis mutandis* to information provided by natural and legal persons making a notification under the preceding Article.

Article 48

Communication to recipients of services

1 - Relevant essential, important and public entities shall report to the recipients of their services, without undue delay, any incidents with a significant impact that are likely to negatively affect them.

2 - Relevant essential, important and public entities shall report to the recipients of their services potentially affected by a significant cyber threat, without undue delay, the measures or solutions that they can adopt to respond to the threat and, where appropriate, communicate to them the cyber threat concerned.

3 - The communication referred to in the preceding paragraph shall not relieve the entities concerned of their duty, at their own expense, to take appropriate and immediate

measures to prevent or remedy any threats and to restore the normal level of security of the service they provide.

4 - The information referred to in the preceding paragraphs shall be provided free of charge and in easily understandable language.

Section III

Incident reporting, public information and response

Article 49

Communication between authorities

1 - Sectoral and special national cybersecurity authorities shall report to the CNCS all incidents of which they are notified in accordance with Article 40, and shall inform the CNCS of their progress.

2 - For the purposes of Article 21, the CNCS shall report to the Secretary-General of the Internal Security System, without undue delay, incidents of which they are notified in accordance with Article 40 that are likely to qualify as large-scale.

3 - The CNCS shall, where it deems it necessary, inform the sectoral and special national cybersecurity authorities of voluntary notifications pursuant to Article 45.

4 - This Article shall apply *mutatis mutandis* to notifications made pursuant to Article 42.

5 - The communications referred to in the preceding paragraphs shall be made immediately by electronic means.

Article 50

Communication to entities within the European Union or its Member States

1 - Where justified, in particular where a significant incident involves at least one other Member State of the European Union, the CNCS shall inform the other affected Member States designated under Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, and ENISA of the occurrence of the same, with the involvement of the cooperation channels on police cooperation and intelligence services.

2 - The communication referred to in the preceding paragraph shall include the information received through the notifications made pursuant to Articles 42 et seq.

3 - The CNCS, as the single point of contact, shall submit a quarterly summary report to ENISA, including anonymised and aggregated data on significant incidents, incidents, cyber threats, and near misses notified pursuant to Articles 40 and 45.

Article 51

Information to the public

1 - The competent cybersecurity authority shall inform the public of the occurrence of a significant incident, after consultation with the entity concerned, where:

a) There is a need for public clarification to prevent the incident or to respond to an ongoing incident;

b) Disclosure of the significant incident is in the public interest.

2 - The competent cybersecurity authority shall also require the entity concerned to disclose the significant incident to the public where the situations referred to in the previous paragraph are concerned.

3 - The competent cybersecurity authority shall inform the public of a significant incident at the request of a competent authority of another Member State of the European Union.

4 - The communication to the public provided for in this Article shall be without prejudice to cooperation in ongoing criminal investigations or those covered by the rules on judicial and State secrecy.

Article 52

Reply to notifications

1 - The competent cybersecurity authority shall reply to the notifying entity without undue delay and, where possible, within 24 hours of receiving the initial notification provided for in Article 42.

Draft Law No .....

2 - The competent cybersecurity authority shall provide in its response, *inter alia*, its initial comments on the significant incident and, at the request of the entity, guidance or operational advice on the implementation of possible mitigating measures.

3 - In situations of serious and proven risk of the impact of the incident notified pursuant to Article 40, the competent cybersecurity authority may impose, as an immediate enforcement measure, the interruption of the provision of service to the relevant essential, important or public entity concerned, or the cessation of conduct that infringes this Decree-Law, if it does not do so on a voluntary basis.

4 - In cases of well-founded suspicion of the criminal nature of the significant incident, the competent cybersecurity authority shall also provide guidance on the notification of the significant incident to law enforcement authorities.

5 - The provisions of the preceding paragraphs shall apply *mutatis mutandis* to incidents, near misses or cyber threats that have been notified on a voluntary basis under Article 45.

Draft Law No .....

Chapter VI

Supervision and enforcement

Section I

Supervisory and enforcement measures

Article 53

Principles

1 - The competent cybersecurity authority, as the supervisory and enforcement authority, shall monitor and supervise compliance with this Decree-Law and take the necessary measures to ensure such compliance.

2 - Supervisory and enforcement activities shall be guided, *inter alia*, by the principles of public interest, legality, efficiency, effectiveness and proportionality and shall minimise, where possible, their impact on the public, social and business activities of the supervised entities.

3 - Supervisory activity shall be based on risk assessment methodologies and, on the basis of that assessment and the principles referred to in the preceding paragraph, may determine the priority allocation of resources and the measures to be taken in accordance with the risk matrix applicable to the entity concerned, in particular as regards the conduct, frequency or type of on-site inspections, targeted

security audits or security checks and the type of information to be requested.

4 - Supervisory and enforcement activities shall be carried out with operational autonomy, including those targeting the relevant public entities.

5 - Supervisory and enforcement activities shall respect the legal and constitutional guarantees of individuals.

Article 54

Supervisory measures concerning essential entities

1 - The competent cybersecurity authority shall have the power to subject essential entities to the following measures:

a) On-site inspections and remote supervision, including random checks by qualified professionals;

b) Regular or targeted security audits carried out by the competent authority itself or, where appropriate, by an entity appropriately qualified for that purpose and offering guarantees of independence;

c) Ad-hoc audits, in particular on the basis of the verification of a significant incident, non-compliance by the competent cybersecurity authority or infringement of this Decree-Law by the entity concerned;

d) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate

in cooperation with the entity concerned;

e) Requests for information necessary to assess compliance with the cybersecurity measures referred to in Articles 27 et seq. adopted by the entity concerned;

f) Requests for access to data, documents and information necessary for the performance of their supervisory tasks;

g) Requests to provide evidence demonstrating the implementation of cybersecurity policies and procedures.

2 - The targeted audits referred to in (1)(b) shall be based on the risk analysis carried out by the competent cybersecurity authority, the risk analysis carried out by the audited entity or other available risk-related information, including those contained in the technical harmonisation instructions and risk matrices prepared by the CNCS pursuant to Article 26(3), as well as the orders, instructions and guidelines of the competent cybersecurity authority.

3 - The costs of targeted audits referred to in p(1)(b) shall be borne by the audited entity, unless the competent cybersecurity authority decides otherwise on a reasoned basis.

4 - Requests for information and evidence referred to in (1) (e) to (g) shall state the purpose of the request, specify the information requested and set an appropriate and reasonable time limit for the essential entity to respond.

Article 55

Draft Law No .....

Supervisory measures concerning relevant important and public entities

1 - Where the competent cybersecurity authority obtains evidence, indications or information that a relevant important or public entity is not complying with this Decree-Law, it shall apply supervisory *ex post* measures provided for in the following paragraphs.

2 - The competent cybersecurity authority shall have the power to subject important entities to the following measures:

a) On-site inspections and remote *ex post* supervision carried out by qualified professionals;

b) Targeted security audits carried out by the competent authority itself or, where appropriate, by an entity appropriately qualified for that purpose and offering guarantees of independence;

c) Ad-hoc audits, in particular on the basis of the verification of a significant incident, non-compliance by the competent cybersecurity authority or infringement of this Decree-Law by the entity concerned;

d) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate in cooperation with the entity concerned;

e) Requests for information necessary to assess compliance with the cybersecurity measures referred to in Articles 27 et seq. adopted by the entity concerned;

f) Requests for access to data, documents and any information necessary for the performance of its supervisory tasks;

g) Requests to provide evidence demonstrating the implementation of cybersecurity policies and procedures.

3 - The targeted audits referred to in (2)(b) shall be based on the risk analysis carried out by the competent cybersecurity authority, the risk analysis carried out by the audited entity or other available risk-related information, including those contained in the technical harmonisation instructions and risk matrices prepared by the CNCS pursuant to Article 26(3), as well as the orders, instructions and guidelines of the competent cybersecurity authority.

4 - The costs of the targeted audits referred to in (2)(b) shall be borne by the audited entity, unless a reasoned decision to the contrary is taken by the competent cybersecurity authority.

5 - Requests for information and evidence referred to in (2)(e) to (g) shall indicate their purpose, specify the information requested, and set an appropriate and reasonable time limit for the essential entity to respond.

Article 56

Implementing measures

1 - The competent cybersecurity authority may, in relation to essential, important and relevant public entities, adopt measures that include the following:

a) Warnings of breaches of the obligations arising from this Decree-Law and the respective applicable regulatory regime;

b) Binding orders or instructions to adopt measures necessary to prevent, deter, or correct an incident, determining the time limits for their execution and reporting;

c) binding orders or instructions to remedy deficiencies or infringements of this Decree-Law;

d) Binding orders or instructions for the purpose of complying with the provisions of Article 26 et seq. or, in the case of a relevant public entity, the provisions of Article 33, or to comply with the provisions of Article 40 et seq.;

e) Orders for the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities potentially affected by a significant cyber threat of the nature of that threat, as well as of any protective or remedial measures that may be taken in response to that cyber threat;

f) Orders for the entity concerned to implement, within a reasonable period of time, the recommendations made as a result of a security audit;

g) The designation of a supervisor with appropriately circumscribed functions, for a limited period of time, to

supervise the compliance of the entity concerned with the obligations laid down in Articles 26 et seq. and Article 40 et seq.;

h) Orders for the entity concerned to publicise the aspects of infringements of this Decree-Law in a specific manner;

i) The imposition of fines in accordance with the following chapter.

2 - In the event of non-compliance by any essential entity with the measures referred to in points (a) to (d) and (f) within the period determined by the competent cybersecurity authority, the competent cybersecurity authority may, to the extent strictly necessary:

a) Suspend a certification, authorisation or licence for some or all of the relevant services provided or activities performed by the entity, or order a certification body to suspend it;

b) Request the competent body to suspend the authorisation or licence for some or all of the relevant services provided or activities carried out by the entity;

3 - The temporary suspensions or disqualifications referred to in the previous paragraph shall continue until such time as the entity remedies the deficiencies or complies with the measures referred to in (1).

4 - The measures referred to in (2) shall not apply to public

entities covered by this Decree-Law, without prejudice to the exercise of management and supervisory powers, in general terms.

Article 57

Blocking and redirection measures

1 - The competent cybersecurity authority may issue orders or instructions to counteract a cyber threat, cyber attack or incident to the network and information systems of the relevant essential, important or public entities resulting from the misuse of domain names or IP protocol addresses, in accordance with the following paragraphs.

2 - The types of abuse referred to in the preceding paragraph include, in particular:

a) Distributed Denial of Service (DDoS) attacks;

b) Malicious servers (Command and Control);

c) Infected equipment (communication with Command and Control);

d) Distribution of malicious code;

e) Illegitimate use of a third party's name;

f) Unsolicited emails (SPAM).

3 - To the extent strictly necessary to stop the misuse of domain names, the competent cybersecurity authority may order, in a duly reasoned manner:

Draft Law No .....

a) The registration of TLD names, requesting the holder of a domain name registration to take appropriate measures, within a specified timeframe, to repress a cyber threat or respond to a cyber attack or incident;

b) The registration of TLD names or DNS service providers, the blocking or redirection of domain names to a secure CNCS server, where they are manifestly dedicated to or involved in cyber-attacks or incidents and no other effective means are available to bring the cyber-attack or incident to an end.

4 - To the extent strictly necessary to stop the misuse of IP protocol addresses, the CNCS may order undertakings providing electronic communications networks and services to block or redirect a dynamic or static IP protocol address to a secure CNCS server where those addresses are manifestly dedicated to or involved in the types of cyber-attacks or incidents referred to in (2)(a) and (d)

5 - The measures referred to in (3) and (4) shall not exceed the period of 60 days, which may be renewed for the same period where there is a strong likelihood, as assessed by a reasoned assessment, that cyber-attacks or incidents originating from the same addresses will persist or be resumed.

6 - The provisions of this Article shall also apply to providers of domain name registration services.

Draft Law No .....

Article 58.

Procedural guarantees

1 - The competent cybersecurity authority shall provide an adequate statement of reasons for its decisions to implement the implementing measures and shall, in general terms, hold a prior hearing of the entity concerned within a reasonable period of time, which shall not be less than 10 days.

2 - The prior hearing referred to in the preceding paragraph shall be waived whenever there is a duly substantiated need for the application of immediate measures to prevent or respond to significant incidents or cyber threats.

3 - When applying any of the implementing measures referred to in the preceding paragraphs, the competent cybersecurity authority shall respect the entity's procedural safeguards, taking into account the circumstances of the individual case, and shall consider, in particular:

a) The seriousness of the infringement and the importance of the provisions infringed;

b) The duration of the infringement;

c) Any previous relevant infringements by the entity concerned:

d) Any material or immaterial damage caused, including any financial or economic loss, the effects on other services and the number of users affected;

e) Any measures taken by the entity to prevent or mitigate

material or non-material damage;

f) The fault of the agent;

g) The level of cooperation of the responsible natural or legal persons with the competent cybersecurity authority.

4 - For the purposes of point (a) of the preceding paragraph, the following shall be presumed to be serious:

a) Repeated breaches of this Decree-Law;

b) Failure to notify incidents in accordance with Articles 40 et seq.;

c) Non-compliance with the duty to correct significant incidents;

d) Non-compliance with the duty to remedy deficiencies following binding instructions from the competent cybersecurity authority;

e) Obstruction of audits or follow-up activities ordered by the competent cybersecurity authority, following the verification of an infringement of this Decree-Law;

f) Provision of false or grossly inaccurate information in relation to the cybersecurity measures set out in Articles 26 et seq. or the notification obligations set out in Articles 40 et seq.

Draft Law No .....

Cooperation between authorities with supervisory powers

Article 59

Incident reporting and application of measures

1 - Sectoral national cybersecurity authorities and special national cybersecurity authorities inform the CNCS of the occurrence of significant incidents or cyber threats, as well as of the implementation of supervisory and enforcement measures on cybersecurity, in accordance with the applicable regime.

2 - The application of supervisory and enforcement measures on cybersecurity, in accordance with the applicable regime, by national sectoral cybersecurity authorities and national special cybersecurity authorities shall be preceded by a non-binding opinion of the CNCS, with the exception, for national sectoral cybersecurity authorities, of the measures provided for in point (i) of Article 56(1).

3 - Sectoral national cybersecurity authorities and special national cybersecurity authorities shall be exempted from requesting an opinion from the CNCS pursuant to the previous paragraph, where compliance with implementing measures is at stake within a period of less than 24 hours, without prejudice to the measures being immediately communicated to the CNCS.

4 - The competent cybersecurity authority shall inform the special national cybersecurity authorities of significant incidents that have occurred and may affect financial sector entities.

5 - The transmission of the above information shall take place through the platform referred to in Article 8(7).

Article 60

Cooperation in the field of critical infrastructure security

1 - Where the CNCS, the sectoral national cybersecurity authorities or the special national cybersecurity authorities, as the case may be, exercise their supervisory powers in respect of an entity referred to in Article 3(5), they shall inform the competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December.

2 - Competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December may, where necessary, request that the CNCS, the national sectoral cybersecurity authorities or the national special cybersecurity authorities, as applicable, exercise their supervisory powers, in relation to an entity referred to in Article 3(5).

Chapter VII

Sanctioning regime

Article 61

Very serious administrative offences

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

1 - The following shall constitute very serious administrative offences under this Decree-Law:

a) Failure to comply with the decisions of the member of the **G**overnment responsible for cybersecurity, as provided for in Article 18(3);

b) Failure to comply with the duty to adopt cybersecurity measures pursuant to Articles 27 to 29;

c) Failure to comply with the obligations laid down in Article 30;

d) Failure to comply with the obligations laid down in Article 31;

e) Failure to comply with the obligations laid down in Article 32;

f) Failure to comply with the duty to adopt the cybersecurity measures established by the CNCS pursuant to Article 33;

g) Failure to comply with the obligations laid down in Article 34;

h) Failure to comply with the obligations laid down in Article 36(1) and (2);

i) Failure to comply with the obligations laid down in Article 37;

j) Failure to comply with the notification obligation pursuant to Articles 40 to 44;

k) Failure to comply with the obligation to report in

accordance with Article 48;

2 - The administrative offences referred to in the preceding paragraph shall be punishable by the following fines:

a) In the case of an essential entity:

i) From EUR 2 500.00 to EUR 10 000 000.00 or 2 % of the total worldwide annual turnover of the essential entity concerned in the preceding financial year, whichever is higher, if carried out by a legal person;

ii) From EUR 500.00 to EUR 250 000.00 if committed by a natural person.

b) In the case of an important entity:

i) From EUR 1 750.00 to EUR 7 000 000.00 or for a maximum amount which shall not be less than 1.4 % of the total worldwide annual turnover of the relevant significant entity in the preceding financial year, whichever is higher, if carried out by a legal person;

ii) From EUR 500.00 to EUR 250 000.00 if committed by a natural person.

c) In the case of a relevant public entity included in Group A referred to in Article 7(2):

i) From EUR 20 000.00 to EUR 5 000 000.00 if

committed by a legal person;

ii) From EUR 750.00 to EUR 20 000.00, if committed by a natural person.

d) In the case of a relevant public entity included in Group B as referred to in Article 7(3):

i) From EUR 10 000.00 to EUR 450 000.00 if committed by a legal person;

ii) From EUR 750.00 to EUR 20 000.00, if committed by a natural person.

Article 62.

Serious administrative offences

1 - The following shall constitute serious infringements under this Decree-Law:

a) Failure to comply with the obligations laid down in Article 8;

b) Failure to comply with the obligations laid down in Article 35;

c) Failure to comply with the obligations laid down in Article 36(4) and (5);

d) Failure to comply with the obligations laid down in Article 46;

e) Failure to comply with the obligation laid down in Article 51(2);

f) Failure to comply with the immediate enforcement measure provided for in Article 52(3);

g) Failure to comply with binding warnings, orders or instructions issued by the competent cybersecurity authority under Article 56(1)(a) to (h);

h) Breach of the suspension determined pursuant to Article 56(2)(a);

i) Breach of the suspension determined pursuant to Article 56(2)(b);

j) Failure to comply with the orders or instructions provided for in Article 57;

2 - The administrative offences referred to in the preceding paragraph shall be punishable by the following fines:

a) in the case of an essential entity:

i) from EUR 1 250.00 to EUR 5 000 000.00 or 1 % of the total worldwide annual turnover of the relevant essential entity in the preceding financial year, whichever is higher, if carried out by a legal person;

ii) From EUR 250.00 to EUR 125 000.00 if committed by a natural person.

b) In the case of an important entity:

i) from EUR 875.00 to EUR 3 500 000.00 or for a maximum amount which shall not be less than 0.7

% of the total worldwide annual turnover of the relevant significant entity in the preceding financial year, whichever is higher, if carried out by a legal person;

ii) From EUR 250.00 to EUR 125 000.00 if committed by a natural person.

c) in the case of a relevant public entity falling within 'Group A' as referred to in Article 7(2):

i) From EUR 10 000.00 to EUR 2 500 000.00 if committed by a legal person;

ii) From EUR 375.00 to EUR 10 000.00 if committed by a natural person.

d) in the case of a relevant public entity belonging to 'Group B' as referred to in Article 7(3):

i) From EUR 5 000.00 to EUR 225 000.00 if committed by a legal person;

ii) From EUR 375.00 to EUR 10 000.00 if committed by a natural person.

Article 63.

Light administrative offences

1 - The following are minor administrative offences:

a) The use, by entities, of an invalid, expired or revoked cybersecurity certification mark;

b) The use of expressions or graphics that expressly or tacitly suggest cybersecurity certification of a product, service, or process that is not certified;

c) Wilful omission of information or provision of false information that is relevant to the ongoing cybersecurity certification process, as defined in each certification regime;

d) Failure to comply with the requests of the Cyberspace Security Assessment Committee provided for in Article 18(7);

e) Failure to comply with the obligations laid down in Article 34.

2 - The administrative offences referred to in the preceding paragraph shall be punishable by the following fines:

a) From EUR 875.00 to EUR 45 000.00, if committed by a legal person;

b) From EUR 250.00 to EUR 3 750.00 if committed by a natural person.

Article 64

Negligence

The administrative offences referred to in Article 61(1), Article 62(1), and Article 63(1)(a) and (b) shall also be punishable by negligence, with the minimum and maximum limits of the fines being halved.

Draft Law No .....

Article 65

Waiver of fines

All relevant essential, important and public entities may, upon a duly reasoned request, request the competent cybersecurity authority to waive the application of fines referred to in Article 61(2) and Article 62(2), on the grounds that there is no internal procedure for adapting those entities to the new legal regime, for 12 months from the entry into force of this Decree-Law.

Article 66

Fixing the amount of the fine

1 - The specific fine is determined on the basis of the seriousness of the specific unlawfulness of the act, the fault of the agent, his economic situation and the economic benefit which he derived from the commission of the administrative offence.

2 - In determining the specific unlawfulness of the act and the fault of the agent, the following circumstances shall be taken into account:

a) The seriousness of the infringement;

b) The duration of the infringement;

c) The occasional or repeated nature of the infringement;

d) The damage caused, including any financial or economic loss, the effects on other services and the number of users

affected;

e) The measures taken by the entity to prevent or mitigate the damage referred to in the previous subparagraph;

f) The level of cooperation of the responsible natural or legal persons with the competent cybersecurity authority.

3 - For the purposes of point (a) of the preceding paragraph, the following shall be presumed to be serious:

a) Repeated breaches of this Decree-Law;

b) Failure to notify incidents pursuant to Articles 40 et seq.;

c) Failure to correct significant incidents;

d) The absence of correction of deficiencies following binding instructions from the competent authorities;

e) Obstruction of audits or follow-up activities ordered by the competent cybersecurity authority, following the verification of an infringement of this Decree-Law;

f) The provision of false or grossly inaccurate information in relation to cybersecurity measures and obligations in relation to cybersecurity measures pursuant to Articles 27 et seq. or notification obligations pursuant to Articles 40 et seq.

4 - The provisions of point (f) of the preceding paragraph shall be without prejudice to liability under the Criminal Code.

5 - Except in case of intent, the initiation of administrative offence proceedings depends on prior warning of the agent, by

the competent cybersecurity authority, to comply with the omitted obligation or reinstatement of the breached prohibition within a reasonable time.

Article 67

Ancillary sanctions and other determinations

Where justified by the seriousness of the infringement and the fault of the infringer, the competent cybersecurity authority may determine, at the same time as the fine:

a) Publication in the Diário da República (Portuguese Official Gazette) and in one of the most widely circulated national, regional or local newspapers, depending on the relevant geographic market, at the offender's expense, of an extract from the conviction decision or, at least, the operative part of the conviction decision issued in the context of proceedings initiated under this Decree-Law, after it has acquired the force of *res judicata*;

b) The prohibition of participation in public procurement procedures, where applicable;

c) The adoption and implementation of a cybersecurity training plan, to be implemented within six months;

d) The adoption or amendment of a security plan, to be implemented within six months;

e) Suspension of the provision of the service until the fulfilment of the omitted duties;

f) Temporary disqualification of the holders of the management, direction and administrative bodies from performing their duties.

Article 68

Compulsory penalties

1 - The addressees of a decision of the competent cybersecurity authority shall be subject to the payment of a sum of money for each day of delay in compliance, counted from the date of its notification.

2 - For the purposes of the preceding paragraph, the imposition on the agent of the payment of a pecuniary amount for each day of non-compliance that occurs beyond the deadline set for compliance with the obligation shall be considered a periodic penalty payment.

3 - The periodic penalty payment shall be set in accordance with criteria of reasonableness and proportionality, the daily amount of the penalty provided for in the preceding paragraph being set at EUR 500.00 when committed by a legal person and at EUR 100.00 when committed by a natural person.

4 - The daily amounts fixed may be increased for each day of non-compliance and may in no case exceed the maximum duration of 30 days.

Article 69

Draft Law No .....

Prescription of the procedure

1 - Proceedings for serious and very serious administrative offences shall be extinguished by prescription as soon as the five-year period has elapsed with regard to the commission of the administrative offence, without prejudice to the causes of interruption and suspension provided for in the general terms.

2 - Proceedings for minor infringements shall be extinguished by the statute of limitations as soon as three years have elapsed since the infringement was committed, without prejudice to the causes of interruption and suspension provided for in the general terms.

Article 70

Limitation period for the fine and ancillary penalties

1 - The limitation period for fines and ancillary penalties shall be:

a) Three years, in the case of serious and very serious administrative offences;

b) Two years in the case of minor offences.

2 - The time limit shall run from the finality or *res judicata* of the conviction.

Article 71

Rule on the competence of the competent authorities

Draft Law No .....

The initiation and investigation of administrative offence proceedings, as well as the application of fines, falls within the competence of the competent cybersecurity authority.

Article 72

Notifications

1 - Notifications by the competent cybersecurity authorities shall be made electronically or, at the reasoned request of the entity, by registered letter or in person.

2 - Electronic notification shall be made by making it available in the digital area reserved for the recipient, integrated into the platform provided for in Article 8(7) and linked to the email address registered therein by the recipient, and also, cumulatively, through the public electronic notification service (SPNE), whenever it is verified that the recipient has joined it, pursuant to Decree-Law No 93/2017 of 1 August, as amended.

3 - The making available shall be accompanied by a notice to the addressee at the email address registered on the platform provided for in Article 8(7), indicating the sending authority and the form of access to the addressee’s reserved area.

4 - Electronic notification shall be deemed to have been made on the date of the electronic consultation of the digital restricted area of the platform provided for in Article 8(7) or, if this does not take place within the first three days of receipt,

on the expiry of that period.

5 - Postal notification shall be deemed to have been effected on the third working day following that of registration.

Article 73

Proceeds from fines

The proceeds of the fines shall accrue to:

a) 60 % to the Government;

b) 40 % to the CNCS or to the relevant national sectoral cybersecurity authority, depending on the entity that initiated and dealt with the case.

Article 74

Costs

1 - For administrative offence proceedings, costs are also due for processing, archiving, and making available.

2 - Decisions of the competent cybersecurity authority on the subject matter of the proceedings shall set the amount of the costs.

3 - Costs are intended to cover the expenses incurred in the proceedings.

4 - Reimbursement for expenses related to notifications and communications, audiovisual media, and materials used in the

proceedings is calculated:

a) Where the process is carried out, in whole or in part, on paper, at a rate of 0.25 UC for the first 50 sheets or fraction thereof and 0.1 UC for each subsequent set of 25 sheets or fraction thereof, without prejudice to the provisions of the following paragraphs;

b) The main proceedings are conducted digitally, up to a maximum of 5 UC, taking into account the complexity of the case and the acts carried out.

5 - The costs also include the following charges:

a) Remuneration of experts, translators, interpreters and technical advisers;

b) Payment due for travel or payments to any entity for the cost of technical services, certificates, or other information and evidence.

6 - If copies or certificates of the case or parts thereof are provided, in physical or digital form, at the request of the accused, an amount calculated in accordance with the same paragraphs shall be added to the amount referred to in the preceding paragraphs.

7 - The costs shall be borne by the accused and jointly and severally liable in accordance with this Decree-Law, in the event of the application of a warning, a fine, or an additional penalty.

8 - The costs shall revert to the CNCS or to the national sectoral cybersecurity authority, depending on the competence to handle

the administrative offence proceedings.

Article 75

Fulfilment of omitted duty

Where the administrative offence results from the omission of a duty, the application of the penalty and the payment of the fine shall not exempt the offender from compliance if this is still possible.

Article 76

Suspension of enforcement of the fine

1 - The competent cybersecurity authority shall suspend the execution of the fine imposed, taking into account the non-repeated nature of the agent’s unlawful conduct, the circumstances of the commission of the infringement and its conduct prior to and subsequent to the crime, whenever it concludes that the mere censorship of the fact, the subjection to ancillary penalties and the threat of a fine adequately and sufficiently achieve the preventive and corrective purposes of the penalty.

2 - The competent cybersecurity authority, if it deems it appropriate to achieve the purposes of the punishment, shall make suspending the execution of the fine subject to compliance with the sanctions and determinations provided for in Article 67, or other duties that it considers relevant.

3 - The conviction decision shall always specify the grounds for suspension and its conditions, including the duration of the suspension.

4 - The period of suspension shall be set between one and three years, from the date of notification of the conviction decision or the final judgment.

Article 77

Repeal of the suspension of the enforcement of the fine

1 - If, during the period of suspension, the convicted person fails to comply with any of the sanctions or determinations provided for in Article 67 or commits a very serious or serious administrative offence, the competent cybersecurity authority shall, after due procedure, revoke the decision to suspend the enforcement of the fine.

2 - The revocation establishes the obligation to pay the fine immediately, without the accused being able to demand compensation for any services rendered or expenses incurred during the previous compliance with the ancillary penalties imposed on him or her.

Article 78

Cancellation of the fine

The fine shall be declared cancelled if, at the end of the period of its

suspension, there are no grounds which could lead to its revocation.

Article 79

Personal data breach

1 - Where the competent cybersecurity authority obtains a reasonable degree of certainty, in the course of supervisory action or enforcement action, that an infringement by an essential or important entity of the obligations laid down in Articles 27 to 29 and Articles 40 to 43 may lead to a personal data breach pursuant to Article 4(12) GDPR, which must be notified pursuant to Article 33 GDPR, it shall, without undue delay, inform the CNPD.

2 - In the event that the CNPD imposes an administrative fine pursuant to Article 58(2)(i) of the GDPR and other applicable national law, the competent cybersecurity authority shall be prevented from imposing an administrative fine as a result of the commission of the same infringement pursuant to this Decree-Law, without prejudice to the provisions of the following paragraph.

3 - The competent cybersecurity authority may impose the implementing measures provided for in Article 56(1)(a) to (h) on essential and important entities whose breach of the obligations under this Decree-Law results in a personal data breach incident.

Draft Law No .....

Article 80

Challenge to the decisions of the competent cybersecurity authority

1 - Without prejudice to the provisions of paragraph 3, if the decision issued by the competent cybersecurity authority in the context of an administrative offence procedure is challenged, it shall forward the respective files to the Public Prosecutor's Office, preferably by electronic means, within 20 working days, and may attach allegations, as well as other elements or information that it considers relevant to the decision in the case, and also offer evidence.

2 - The sending of the file by electronic means dispenses with the sending of the respective originals, without prejudice to the obligation to submit the procedural documents in paper form and the originals of the documents contained therein, where they exist, whenever the Public Prosecutor's Office or the judge so determines.

3 - Decisions or any measures adopted and implemented by the competent cybersecurity authority in the context of administrative offence proceedings may be challenged before the Competition, Regulation and Supervision Court, and the appeal must be submitted to the competent cybersecurity authority.

4 - The challenge to any decisions issued by the competent cybersecurity authority that, in the context of administrative offence proceedings, determine the imposition of fines or ancillary penalties shall have suspensive effect.

Draft Law No .....

5 - Challenges to other decisions or measures of the competent cybersecurity authority, including decisions imposing periodic penalty payments, adopted in the context of administrative offence proceedings, shall have a purely devolutive effect and shall comply with the rules laid down in this Article.

6 - The competent cybersecurity authority, the Public Prosecutor's Office and defendants may object to the court ruling by order without a trial hearing.

7 - In an appeal against a decision handed down in administrative offence proceedings, the withdrawal of the indictment by the Public Prosecutor’s Office depends on the agreement of the competent cybersecurity authority.

8 - The competent cybersecurity authority shall have the right to appeal autonomously against any judgments and orders that are not merely procedural, including those relating to nullities and other preliminary or incidental questions, or to the application of precautionary measures, as well as to respond to appeals lodged.

9 - Decisions of the *Tribunal da Concorrência, Regulação e Supervisão* (Competition, Regulation and Supervision Court) that allow appeals, in accordance with the general rules on administrative offences, may be challenged before the T*ribunal da Relação de Lisboa* (Lisbon Court of Appeal).

10 - The Court of Appeal, within the jurisdiction provided for in the preceding paragraph, shall rule in the last instance, and

there shall be no ordinary appeal against its judgments.

Article 81

Subsidiary law

In matters relating to administrative offences, in all matters not provided for in this Decree-Law, the provisions of the General Regime of the Illicit Mera Ordenação Social, approved by Decree-Law No 433/82 of 27 October 1982, as amended, shall apply on a subsidiary basis.

Chapter VIII

Supplementary Provisions

Section I

Other provisions

Article 82

Supervision fee

1 - Essential and important entities may be charged a supervisory fee in return for the supervisory acts carried out, to be set on the basis of the costs necessary for the provision of supervisory services.

2 - Supervisory fees shall comply with the principle of

proportionality and shall be set in accordance with objective and transparent criteria.

3 - The regime governing the fees referred to in the preceding paragraphs shall be established by order of the members of the Government responsible for the areas of finance and cybersecurity.

Article 83

Communications

1 - Communications between entities with the CNCS, or with the national sectoral cybersecurity authorities referred to in point (a) of paragraph 2 of Article 15, including incident notifications pursuant to Articles 40 et seq., shall follow the format and procedure defined by the CNCS in a regulation to be approved by the CNCS.

2 - In the absence of any applicable regulatory provision, all communications addressed to the competent cybersecurity authority within the scope of this Decree-Law, as well as the sending of information, shall be carried out by electronic means.

3 - In cases where the entity temporarily does not have the operational capacity to ensure the communication provided for in the preceding paragraphs, or in cases where the Internet website of the competent cybersecurity authority is unavailable as a result of the incident or for another duly justified

eminently technical reason, the notification may exceptionally be made by e-mail or by telephone.

4 - The format and procedure referred to in paragraph 1 shall be adopted by the CNCS, following prior consultation with the relevant sectoral national cybersecurity authorities, which may also adopt their own formats and procedures, adapted to their specificities, as referred to in paragraph 1.

5 - The cases referred to in paragraph 3 shall be subject to technical instructions from the CNCS, adopted in liaison with the sectoral national cybersecurity authorities.

Article 84

Information security and integrity

1 - The CNCS and the relevant sectoral national cybersecurity authorities pursuant to point (a) of Article 15(2) maintain and manage security and integrity information in a secure information system, in accordance with the provisions relating to the security of classified materials at national level and within the framework of the international organisations to which Portugal is a party.

2 - Access to electronic systems and Internet websites for processing the notifications provided for in this Decree-Law shall preferably be carried out using an electronic identification system with a high level of assurance, as defined in Articles 8 and 9 of Regulation (EU) No 910/2014 of the

Draft Law No .....

European Parliament and of the Council of 23 July on electronic identification and trust services, in particular by means of the Citizen's Card and the Digital Mobile Key, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024.

Chapter IX

Transitional and final provisions

Article 85

Approval of the national plan for responding to large-scale cybersecurity incidents and crises

The Plan referred to in Article 13 shall be approved within six months of the entry into force of this Decree-Law.

Article 86

Allocation of resources and operational independence of the CNCS

In order to carry out the tasks and exercise the powers provided for in this Decree-Law, the CNCS must be provided with the necessary resources and enjoy operational independence from the supervised entities.

Draft Law No .....

Article 87

Interoperability and access to information

1 - The CNCS shall have free access to the relevant national databases and registers for the performance of the tasks and exercise of the powers provided for in this Decree-Law and other legislation on cybersecurity, in particular for the attribution or confirmation of the qualification of entities.

2 - The public authorities responsible for the national databases and registers referred to in the preceding paragraph shall provide access to them by means of an interoperability solution laid down in a protocol and appropriate for that purpose.

3 - Failure to sign the protocols referred to in the preceding paragraph shall not prevent access to the relevant information by the CNCS, and the public entities responsible for the national databases and registers shall provide all the necessary information whenever requested by the CNCS.

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

ANNEX I

(referred to in Articles 3, 6, 12 and 35)

Critical sectors

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	Electricity undertakings within the meaning of Article Point 57 of Article 2 of Directive (EU) 2019/944 of the European Parliament and of the Council of the European Parliament and of the Council, which exercise the activity of marketing within the meaning of Article 2(12) of that Directive
		Distribution system operators within the meaning Article 2, point (29), of Directive (EU) 2019/944
		Transmission system

Draft Law No .....

		operators within the meaning of Article 2, point (35), of Directive (EU) 2019/944
		producers as defined in point (38) of Article 2, of Directive (EU) 2019/944
		Nominated electricity market operators as defined in Article 2, point 8, of the Regulation (EU) 2019/943 of the European Parliament and of the Council
		Market participants within the meaning of Article Article 2, point (25), of Regulation (EU) 2019/943, providing aggregation and response services demand for or storage of energy in the as defined in points (18), (20),

Draft Law No .....

		and (59) of Article 2 of Directive (EU) 2019/944
		Operators of a recharging point who are responsible for the management and operation of a recharging point providing a charging service to end-users, including in the name and on behalf of a provider mobility services
	(b) Systems for heating and cooling urban	District heating system operators or district cooling systems within the meaning of Article 2(19) of Directive (EU) 2018/2001 of the European Parliament and of the Council
	(c) Petroleum	Oil pipeline operators
		Production and refining plant operators

		and processing, storage and transport of oil
		Central storage entities within the meaning Article 2(f) of Directive 2009/119/EC the Council
	(c) Gas	Marketing companies within the meaning of Article 2(8) of Directive 2009/73/EC of the European Parliament and of the Council
		Distribution system operators within the meaning point 6 of Article 2 of Directive 2009/73/EC
		Transmission system operators within the meaning point (4) of Article 2 of Directive 2009/73/EC
		Storage system operators

Draft Law No .....

		as defined in Article 2, point 10, of the Directive 2009/73/EC
		LNG network operators within the meaning of Article Point 12 of Article 2 of Directive 2009/73/EC
		Natural gas undertakings within the meaning of Article Point 1 of Article 2 of Directive 2009/73/EC
		refinement facility operators and natural gas treatment
	(e) Hydrogen	Production, storage and hydrogen transport
2. Transports	a) Air transport	Air carriers within the meaning of Article Point 4 of Article 3 of Regulation (EC) No 300/2008 used for commercial purposes
		Airport managing bodies within the meaning of

Draft Law No .....

		Article 2(2) of Directive 2009/12/EC of the European Parliament European Parliament and Council, airports in the as defined in point (1) of Article 2 of that Directive, including the main airports listed Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council, and entities operating installations Auxiliaries existing within airports
		Air traffic management control operators providing traffic control services airborne (CTA) within the meaning of point (1) of Article 2 of

Draft Law No .....

		Regulation (EC) No 549/2004 of the European Parliament European Parliament and Council
	b) Rail transport	Infrastructure managers within the meaning of Article Article 3(2) of Directive 2012/34/EU of the European Parliament and of the Council European Parliament and Council
		railway undertakings within the meaning of Article 3, point 1 of Directive 2012/34/EU, including the operators of service facilities within the meaning of Article 3(12) of that Directive
	c) Water transport	Waterway transport companies inland, maritime and coastal passengers and goods, as defined for the maritime transport in Annex I

		to the Regulation (EC) No 725/2004 of the European Parliament and of the Council, excluding vessels operated by these companies
		Managing bodies of ports within the meaning of Article 3(1) of Directive 2005/65/EC of the European Parliament and of the Council, including their port facilities within the meaning of Article 2(11) of Regulation (EC) No 725/2004, and the entities managing the works and existing equipment within ports
		Operators of maritime traffic services (VTS, from English, vessel

Draft Law No .....

		traffic services) within Article 3 of Directive 2002/59/EC of the European Parliament and of the Council
	d) Road transport	Road authorities within the meaning of Article Article 2(12) of Delegated Regulation (EU) Commission Implementing Regulation (EU) 2015/962, responsible for traffic management control, with the exception of public entities in which the management of the traffic or the management of transport systems Smart devices are a non-essential part of its general activity
		Intelligent transport system operators within the meaning of Article

Draft Law No .....

		4(1) of the Directive 2010/40/EU of the European Parliament and of the Council
3. Banking sector		credit institutions, as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council
4. Infrastructure of the market financial		Operators of trading venues as defined in Article 4(24) of Directive 2014/65/EU of the European Parliament and of the The Council
		Central counterparties (CCPs) within the meaning of Article Article 2(1) of Regulation (EU) No 648/2012 of the European Parliament and of the Council
5. Health		Healthcare providers within the meaning Article 3(g) of Directive

		2011/24/EU of the European Parliament and of the Council
		EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament European Parliament and Council
		Entities carrying out research activities and development of medicinal products in the as defined in point (2) of Article 1 of Directive 2001/83/EC Regulation (EC) of the European Parliament and of the Council
6. potable water		Suppliers and distributors of water intended for human consumption within the meaning of Article

Draft Law No .....

		2 (1)(a) of Directive (EU) 2020/2184 of the European Parliament and of the Council, excluding distributors for whom the distribution of drinking water constitutes a part non-essential to its general distribution activity of other basic products and goods
7. Waste Water		Companies that collect, dispose of or treat urban waste water, domestic waste water or industrial waste water as defined in Article 2(1), (2) and (3) of Council Directive 91/271/EEC of the Council, excluding the undertakings for which the

		collection, disposal or urban and domestic waste water treatment The industrial sector is not a part of essential to its general activity
8. Digital infrastructure		Traffic exchange point providers
		DNS service providers, excluding root name server operators
		TLD name registries
		Computing service providers in cloud
		Data centre service providers
		Content distribution network providers
		Trust service providers
		Providers of public communications networks electronic

Draft Law No .....

		Electronic communications service providers accessible to the public
9. Management of ICT services (between companies)		Managed service providers
		Managed security service providers
10. Room space		Land infrastructure operators, owned, managed and operated by Member States or private entities, which support the provision of space services, excluding providers of public electronic communications networks

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

ANNEX II

(referred to in Articles 3, 6, 12 and 35)

Other critical sectors

Sector	Subsector	Type of entity
1. Postal services and courier		Postal service providers within the meaning of Law No 17/2012 of 26 April, as amended, including courier service providers
2. Management of Waste		Companies carrying out waste management as defined in Article 3(9) of the Directive 2008/98/EC of the European Parliament and of the Council, but excluding enterprises for which waste management does not constitute the activity main economic activity
3. Production manufacturing and distribution		Companies carrying out the production of substances and the distribution of substances or mixtures referred to

of products chemicals		Article 3(9) and (14) of the Regulation (EC) No 1907/2006 of the European Parliament and of the Council and companies carrying out the production 'articles' within the meaning of Article 3(3) of same regulation, of substances or mixtures
4. Production Transformation and distribution of products food		Food businesses within the meaning of Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council, which engage in wholesale distribution and production and industrial processing
5. Manufacturing	(a) Manufacture of devices doctors and devices	Entities manufacturing medical devices in the as defined in point (1) of Article 2 of the Regulation (EU) 2017/745 of the European Parliament and of the Council, and entities that

	Doctors for in vitro diagnostic	manufacture devices in vitro diagnostic medical devices within the meaning of Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council, with the exception of entities that manufacture medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of equipment computer systems, equipment for communication, products electronic	Undertakings carrying out any of the activities economic activities referred to in Section C, Division 26 of NACE Rev. 2

	and optical	
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the activities economic activities referred to in Section C, Division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment (not specified)	Undertakings carrying out any of the activities economic activities referred to in Section C, Division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the activities economic activities referred to in Section C, Division 29 of NACE Rev. 2
	(f) Manufactur	Undertakings carrying out any of the

Draft Law No .....

	e of other equipment transport	activities economic activities referred to in Section C, Division 30 of NACE Rev. 2
6. Provision of digital services		Providers of online marketplaces
		Search engine service providers Straight
		Service platform providers of social networks
7. Investigation		Research organisations

Draft Law No .....

ANNEX III

(referred to in Articles 3, 6, 7 and 12)

Article 1

Company:

An undertaking is any entity engaged in an economic activity, irrespective of its legal form. In particular, entities engaged in artisanal or other activities on an individual or family basis, partnerships or associations regularly engaged in an economic activity shall be regarded as such.

Article 2

Categories

1 - The category of micro, small and medium-sized enterprises (SMEs) consists of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, or an annual balance sheet total not exceeding EUR 43 million.

2 - In the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million.

3 - In the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover or annual balance sheet total does not exceed EUR 2 million.

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

PRESIDENCY OF THE COUNCIL OF MINISTERS

.....

Draft Law No .....

Form

Proposal for an authorisation law

Way:

Office Responsible:

Office of the Minister of the Presidency

a) Summary to be published in *Diário da República*:

Authorises the Government to transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures for a high common level of cybersecurity across the Union by approving the cybersecurity legal regime.

b) Justification of the proposed form of the project:

This is a proposal for an authorisation law, in accordance with Article 198(1)(b) of the Constitution, because it concerns the relative competence of the AR under Article 165(1)(b) of the Constitution. In the case of matters falling within the relative competence of the Assembly of the Republic, the Government may legislate only with the authorisation of the Assembly of the Republic.

c) Current legal regime and basis for its amendment:

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December laying down measures for a high common level of cybersecurity across the Union.

Draft Law No .....

d) Summary and justification of the act, including in particular the identification of the main policy measures:

Summary and justification of the act in accessible language	Authorises the Government to transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures to ensure a high common level of cybersecurity across the Union.
Main measures	The regime approved by the Decree-Law authorised by this draft law significantly expands the range of entities covered by the regime, prioritising, on the one hand, the generalisation of cybersecurity risk prevention, but graduating the regulatory requirement according to the size of the entity and the importance of its activity, as well as privileging the proportionality of the applicable measures. Its scope covers a significant part of the public administration, adapting the regime to the size and typology of the public entity concerned. It should also be noted that, as permitted by the Directive to be transposed, the regime approved by the authorised Decree-Law excludes from its scope public entities in the fields of national security, public security, defence and

Draft Law No .....

	intelligence services. Among the relevant aspects of the regime approved by the authorised Decree-Law is also the deepening of three fundamental instruments for public cybersecurity policies: the National Cybersecurity Strategy, defining national cybersecurity priorities and strategic objectives; the National Plan for Crisis Response and Large-Scale Cybersecurity Incidents, regulating and improving the management of such incidents; and the National Cybersecurity Reference Framework, which will bring together and enable the dissemination of norms, standards and best practices in cybersecurity management. Moreover, the institutional framework of the regime approved by the authorised Decree-Law is extended in relation to the previous regime, as required by the Directive to be transposed In this regard, the National Cybersecurity Centre (CNCS) strengthens its role as the national cybersecurity authority, with the establishment of 'sectoral' and 'special' supervisory authorities exercising supervision over specific sectors of the economy also being highlighted, thus ensuring

	stability in the supervision of each of the sectors covered, as well as alleviating the cross-cutting tasks entrusted to the CNCS. At the inter-administrative level, the proposed model establishes an architecture of convergence, cooperation, and interoperability between the various national entities responsible for cybersecurity and internal and external security, promoting, in particular, the transversality of relevant information flows and the sharing of tactical contributions in incident response between the national entities responsible for cybersecurity, with a view to maximising Portuguese public capabilities for the prevention, early detection, mitigation, prosecution and accountability of cyber threats. Strengthening cooperation with the private sector is another of the axes of the institutional design provided for in the regime approved by the authorised Decree-Law, fostering collaboration between the competent authorities and the private sector **in the various** relevant matters. As for the risk management model provided

	for in the regime approved by the authorised Decree-Law, it consists of the establishment of predefined risk standards applicable to each sector and type of entity, and the application of corresponding prevention measures, plus an analysis of the residual risk. This model relieves authorities of a case-by-case analysis of the risk of each covered entity, and facilitates covered entities in identifying the category to which they belong and, consequently, the minimum measures they must adopt. Accordingly, the proposed model introduces simplicity, predictability, and better alignment of mandatory measures with the threat framework applicable to each sector of activity. On the other hand, the model fosters the creation of a cybersecurity certification market, which will have economic utility and will allow for the generalisation of a presumption of conformity of entities. Finally, as regards the supervisory model provided for in the regime approved by the authorised Decree-Law, this, reflecting the provisions of the Directive to be transposed, provides for a dual regime, differentiating the treatment to be given to essential and important entities according to the

	cybersecurity risks associated with each category, in compliance, once again, with the principle of proportionality.
Key/critical points	

e) Relation to the Government Programme:

Yes	Identification of the concrete measure: 6.4.2. Cyber security Form consensus on a revision of the National Cybersecurity Strategy and properly adopt the European Directive in this area (NIS2), with the aim of promoting a resilient digital nation.

f) Relationship with European funds:

No	
Deadline:	

g) Proposed press release:

It transposes Directive (EU) 2022/2555 of the European

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Parliament and of the Council of 14 December on measures for a high common level of cybersecurity across the Union.

h) Need for internal opinions or external consultations, carried out or to be carried out:

1. Mandatory internal opinions:

[fill in with a '*X*' in the applicable table(s)] Insert dates in the format 'DD-MM-YYYY']

Entities	Yes	No	Home	End	Comm.
Minister for State and Foreign Affairs	X				
Minister for State and Finance	X				
Minister of the Presidency		X			

Draft Law No .....

2. Hearings to be held after deliberation in RSE (identify):

Obligatory	Optional	Home	End	Entity	Standard requiring consultation (mandatory consultations)

[add or delete lines as needed] Insert dates in the format 'DD-MM-YYYY']

i) Specific identification of the legislation to be amended or repealed:

[add or delete lines as needed]

Legislation to be amended, with all amendments made in the meantime	Legislation to be repealed
Internal Security Law, approved by Law No 53/2008 of 29 August, as amended by Law No 59/2015 of 24 June, by Decree-Law No 49/2017 of 24 May, by Laws No 21/2019 of 25 February	Articles 60 to 65 and points (m) to (t) of Article 178(3) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as

Draft Law No .....

and 73/2021 of 12 November, by Decree-Law No 122/2021 of 30 December, by Law No 24/2022 of 16 December and by Decree-Laws No 41/2023 of 2 June and 99-A/2023 of 27 October; Cybercrime Law, approved by Law No 109/2009 of 15 September, as amended by Law No 79/2021 of 24 November.	amended; The Cyberspace Security Legal Regime, approved by Law No 46/2018 of 13 August; Regulation of the Cyberspace Security Legal Regime, approved by Decree-Law No 65/2021 of 30 July, Article 2(2) and Articles 2-A and 6-A of Decree-Law No 3/2012 of 16 January, as amended, approving the organisation of the National Security Office.

j) Express identification of possible complementary legislation, including regulatory instruments:

[add or delete lines as needed]

Complementary regulatory act(s) and other compulsory subordinate act(s)	Does(Do) it(they) accompany the project?	Elements of the regulatory draft(s)

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Ordinance of the member of the Government responsible for cybersecurity to approve the list of essential, important, and relevant public entities; Resolution of the Council of Ministers to approve the National Cybersecurity Strategy; Resolution of the Council of Ministers approving the National Plan for Response to Large-Scale	N	Summary: Competent Authority: Way:

Draft Law No .....

Cybersecurity Incidents and Crises. Ordinance of the Member of the Government responsible for cybersecurity approving the National Cybersecurity Reference Framework. Decree-Law regulating the supervisory fee that aims to remunerate the specific costs of the competent cybersecurity authority.		

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Additional regulations to be adopted by the CNCS.		

k) Summary assessment of the financial and human resources needed for implementation in the short and medium term, as well as of new administrative acts needed:

1. Financial resources involved:

Maintains?	Effect on revenue	Effect on expenditure
Yes		

2. Human resources involved:

Maintains?	Increases	Decreases
Yes		

3. New administrative act(s) required:

Yes	No

Draft Law No .....

Which?	[X]
It involves an increase in costs or other charges for companies. In what way?	

l) Consideration of the advisability of setting up an exemption regime for micro, small and medium-sized enterprises or, failing that, a specific regime that takes account of the specific characteristics of these enterprises and mitigates the impact of these charges:

Yes	The legislation provides for a specific regime that takes into account the particularities of these companies and mitigates the impact of the said charges.
No	

m) Legislative impact indicators, where applicable, including:

1. Economic and competitive impact assessment

Yes	It is foreseen in the applicable regulatory and supervisory regime on cybersecurity.
No	Why?

2. Impact assessment on the risks of fraud, corruption and

Draft Law No .....

related offences

Yes	
No	Why?

3. Impact assessment on disability

Yes	
No	Why?

4. Poverty impact assessment

Yes	
No	Why?

5. Evaluation of the impact on non-discrimination policies on the grounds of descent, sex, race, language, territory of origin, religion, political or ideological beliefs, education, economic situation, social condition or sexual orientation (Article 13(2) of the Portuguese Constitution)

Yes	
No	Why?

6. Assessment of the impact on family and natality policies

Yes	

Draft Law No .....

No	Why?

n) Identification of the EU legal act to be transposed and/or implemented, where applicable:

1. Transposition and/or implementation of an EU legislative act

How much?

Yes:	Which: It transposes Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures for a high common level of cybersecurity across the Union.
Is compliant or performs European obligations	Which?
May not be compatible	Why?
No	[X]

2. Correlation table (Article 33(2) of Annex I to RCM No 65/2024)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Article	National transposition
Article 1 Subject 1. This Directive lays down measures aimed at achieving a high common level of cybersecurity across the Union with a view to improving the functioning of the internal market. 2. To that end, this Directive establishes: (a) The obligation for Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact for cybersecurity (single points of contact), and computer security incident response teams (CSIRTs); (b Cybersecurity risk-management	Article 1 Subject 1 - This Decree-Law establishes the Cybersecurity Legal Regime, transposing into national law Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 1 Directive). 2 - The provisions of this Decree-Law shall

) measures and notification obligations for entities of the type referred to in Annex I or II, as well as for entities identified as critical entities pursuant to Directive (EU) 2022/2557; (c) Rules and obligations on cybersecurity information sharing; (d) Supervisory and enforcement obligations for Member States.	be without prejudice to compliance with the provisions of the applicable legislation on: a) Criminal investigation proceedings by the competent judicial authorities and criminal police bodies, in particular the Public Prosecutor's Office and the Criminal Police; b) Processes falling within the exclusive competence of the Security Intelligence Service and the Strategic Defence Intelligence Service in relation to the production of information relating

Draft Law No .....

	to the safeguarding of national independence, national interests, the external and internal security of the Portuguese State, and the prevention of sabotage, terrorism, espionage and the commission of acts which, by their nature, may alter or destroy the constitutionally established rule of law; g) Protection of personal data, in particular within the scope of the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August, and Law No

Draft Law No .....

	59/2019 of 8 August; h) Identification and designation of national and European critical infrastructures, in particular under Decree-Law No 20/2022 of 28 January; i) Combating the sexual abuse and sexual exploitation of children and child pornography, in particular under Law No 103/2015 of 24 August; j) Protection of users of essential public services, in particular under the **Electronic Communications Law, approved by Law** No 23/96 of 26

Draft Law No .....

	July, as amended; k) Security and emergency in the electronic communications sector, in particular under the provisions of Law No 16/2022 of 16 August, as amended; l) State Secrets and Classified Information, in particular under the provisions of Organic Law No 2/2014 of 6 August, as amended.
Article 2 Scope of application 1. This Directive shall apply to public or private entities of one of the types referred to in Annex I or II which are considered to be medium-sized enterprises in	Article 3 Subjective scope 1 - This Decree-Law shall apply to private entities of one of the types listed in Annexes

accordance with Article 2 of the Annex to Recommendation 2003/361/EC, or exceeding the thresholds for medium-sized enterprises set out in paragraph 1 of that article, and who provide their services or carry out their activities in the Union. Article 3(4) of the Annex to that Recommendation does not apply for the purposes of this Directive. 2. Irrespective of their size, this Directive shall also apply to entities of a type referred to in Annex I or II, where: (a) The services are provided by: (i) Providers of public electronic communications networks or providers of publicly available electronic communications services; ii) Trust service providers; iii) Top-level domain name	I or II to this Decree-Law which, respecting the territorial scope criteria set out in the following Article: *a)* Are qualified as medium-sized enterprises in accordance with Article 2 of Annex III to this Decree-Law, corresponding to that provided for in Commission Recommendation 2003/361/EC of 6 May, or exceed the thresholds for medium-sized enterprises provided for in paragraph 1 of that Article; and *b)* Provide their services or carry out their activities in the European Union.

Draft Law No .....

) registries and domain name system service providers; (b) The entity is the only provider in a Member State of a service that is essential for the maintenance of critical societal or economic activities; (c) A disruption of the service provided by the entity could significantly affect public security, public protection or public health; (d) A disruption of the service provided by the entity could generate considerable systemic risks, especially for sectors where such disruption could have a cross-border impact; (e) The entity is critical because of its specific importance, at national or regional level, for the	2 - This Decree-Law shall also apply to entities of one of the types listed in Annexes I or II to this Decree-Law which, irrespective of their nature and size and in compliance with the territorial scope criteria laid down in the following Article, meet at least one of the following requirements: *a)* The entity concerned is: *i)* A provider of public electronic communications networks or provider of publicly available electronic communications services; *ii)* A trust service provider;

sector or type of service concerned, or for other interdependent sectors in the Member State; (f) The entity is a government entity: (i) Central government, as defined by a Member State in accordance with national law, or (ii) At regional level, as defined by a Member State in accordance with national law, which, following a risk-based assessment, provides services the disruption of which would be likely to have a significant impact on critical societal or economic activities. 3. Irrespective of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557. 4. Irrespective of their size, this	*iii)* Top-level domain name registration, domain name registration service provider, and domain name system service provider. *b)* The entity concerned is the only provider of a service that is essential for the maintenance of critical social or economic activities, including activities corresponding to the sectors, subsectors and types of entities referred to in Annexes I and II to this Decree-Law; *c)* A disruption of the service it provides could significantly

Draft Law No .....

Directive shall apply to entities providing domain name registration services. 5. Member States may provide that this Directive applies to: (a) Public administration entities at local level; (b) Educational institutions, in particular when carrying out critical research activities. 6. This Directive is without prejudice to the responsibilities of the Member States to safeguard national security and their powers to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order. 7. This Directive shall not apply to public administration entities carrying out their activities in the areas of national security, public security, defence or law enforcement, including the	affect public security, public protection or public health; *d)* A disruption of the service it provides may generate considerable systemic risks, especially for sectors for which such disruption may have a cross-border impact; *e)* The entity is critical due to its specific importance, at national or regional level, for the sector or type of service concerned, or for other interdependent sectors. 3 - This Decree-Law applies to the Public Administration, covering:

Draft Law No .....

prevention, investigation, detection and prosecution of criminal offences. 8. Member States may exempt specific entities which carry out activities in the fields of defence, national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which offer services exclusively to public administration entities referred to in (7) of this Article, to comply with the obligations set out in Article 21 or 23 with regard to those activities. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply to those specific activities or services. Where entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may also decide to exempt such entities from the obligations laid down in Articles	*a)* Direct State administration services, central and peripheral; *b)* Direct administration services of the Autonomous Regions, central and peripheral; *c)* Entities of the indirect administration of the State; *d)* Indirect administration entities of the Autonomous Regions; *e)* Self-governing entities; *f)* Independent administrative bodies and entities, with the exception of the Banco de Portugal, the

Draft Law No .....

3 and 27. 9. (7) and (8) do not apply when an entity acts as a trust service provider. 10. This Directive shall not apply to entities that Member States have excluded from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that regulation. 11. The obligations laid down in this Directive shall not entail the provision of information the disclosure of which would be contrary to the essential interests of the Member States relating to national security, public security or defence. 12. This Directive shall apply without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU and 2013/40/EU of the European Parliament and of the Council and Directive (EU) 2022/2557. 13. Without prejudice to Article	Securities Market Commission, and the Insurance and Pension Funds Supervisory Authority. 4 - This Decree-Law shall apply to the following entities: a) Ombudsman; b) Economic and Social Council; c) Technical and administrative services of the Presidency of the Republic, the Assembly of the Republic, the Courts and secretariats with competence for the processing of procedures, the High Council of the Judiciary, the High Council of

Draft Law No .....

346 of the TFEU, information classified as confidential pursuant to Union or national rules, such as rules on business confidentiality, may be exchanged with the Commission and other competent authorities in accordance with this Directive only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to what is relevant and proportionate to the purpose of the exchange. The exchange of information shall preserve the confidentiality of that information and safeguard the security and commercial interests of the entities concerned. 14. Entities, competent authorities, single points of contact and CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular on the basis of Article 6 of that regulation.	Administrative and Fiscal Courts, and the High Council of the Public Prosecution Service, without prejudice to (6). 5 - This Decree-Law shall apply to entities that, irrespective of their size, are identified as critical entities pursuant to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December on the resilience of critical entities, without prejudice to (3)(f). 6 - This Decree-Law shall not apply: a) To the General Staff of the Armed Forces and of the branches of the Armed Forces, as regards network

Any processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in compliance with Union data protection law and Union law on privacy, in particular Directive 2002/58/EC.	and information systems directly related to their command and control; b) To public entities with criminal investigation responsibilities and criminal police and public security bodies, as regards network and information systems directly related to their command and control; c) To public entities with exclusive responsibilities for the production of information, in particular the Information System of the Portuguese Republic, the Strategic Defence

Draft Law No .....

	Information Service, and the Security Intelligence Service, as regards network and information systems directly related to their command and control; d) To public entities whose activity concerns network and information systems directly related to the production and dissemination of classified information, including national, NATO, and European Union trademarks, or catalogued as a State Secret, with regard to such network and

	information systems; e) To other public entities operating in the fields of national security, public security, defence, and intelligence with regard to network and information systems directly related to the activities of intelligence generation and the prevention, investigation, detection and prosecution of criminal offences; f) Private entities providing services exclusively to one or more of the entities referred to in the preceding points and in respect of these

Draft Law No .....

	activities. 7 - This Decree-Law shall apply to the entities referred to in Article 15(2) (b) only as regards the exercise of their competences as special national cybersecurity authorities. 8 - This Decree-Law is without prejudice to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December on digital operational resilience for the financial sector.
Article 3 Essential and important entities 1. For the purposes of this Directive, the following entities shall be considered essential entities:	Article 6 Essential entities and important entities 1 - For the purposes of this Decree-Law, the following shall be

Draft Law No .....

(a) Entities of a type referred to in Annex I exceeding the thresholds for medium-sized enterprises set out in Article 2(1) of the Annex to Recommendation 2003/361/EC;	considered essential entities: a) Entities of one of the types referred to in Annex I to this Decree-Law that exceed the thresholds provided for in Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May;
(b) Qualified trust service providers and TLD name registries, as well as DNS service providers, regardless of their size;	b) Providers of qualified trust services and top-level domain name registration, and providers of domain name systems, regardless of their size;
(c) Providers of public electronic communications networks or providers of publicly available electronic communications services that qualify as medium-sized enterprises in accordance with Article 2 of the Annex to Recommendation 2003/361/EC;	c) Undertakings providing public
(d) Government entities referred to in Article 2(2)(f)(i);	
(e) any other entity of a type referred to in Annex I or II that a	

Member State has identified as an essential entity pursuant to Article 2(2)(b) to (e); (f) Entities identified as critical entities pursuant to Directive (EU) 2022/2557 as referred to in Article 2(3) of this Directive; (g) Where the Member State so provides, entities that the Member State concerned has identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law. 2. For the purposes of this Directive, entities of one of the types referred to in Annex I or II which are not considered essential entities shall be considered to be important entities under (1) of this Article. This includes entities identified by Member States as important entities pursuant to Article 2.(2)(b) to (e).	electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises in accordance with Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May; d) Public Administration entities whose tasks include the provision of services in the areas of development, maintenance, and management of information and communication

Draft Law No .....

3. By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years. 4. For the purpose of establishing the list referred to in (3), Member States shall require the entities referred to in that paragraph to submit to the competent authorities at least the following information: (a) Entity name; (b) The up-to-date address and contact details, including e-mail addresses, IP address ranges and telephone numbers; (c) Where applicable, the relevant sector and subsector referred to	technology infrastructures, or those with a particularly high degree of digital integration in the provision of their services, identified and qualified in accordance with Article 8; e) Entities identified as critical entities pursuant to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December on the resilience of critical entities and repealing Council Directive 2008/114/EC, irrespective of their size;

in Annex I or II; and (d) Where applicable, a list of Member States in which they provide services falling within the scope of this Directive. The entities referred to in (3) shall notify without delay any changes to the data provided pursuant to the first subparagraph of this paragraph and in any event within two weeks from the date of the change. The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall, without undue delay, provide guidelines and templates with regard to the obligations set out in this paragraph. Member States may establish national mechanisms allowing entities to register themselves. 5. By 17 April 2025 and every two years thereafter, competent	f) Any other entity of a type listed in Annexes I or II to this Decree-Law, referred to in Article 3(2)(b) to (e), which qualifies as an essential entity based on the respective degree of exposure of the entity to risks, the size of the entity, and the probability of occurrence of incidents and their severity, including their social and economic impact. 2 - For the purposes of this Decree-Law, important entities are entities of the types referred to in Annexes I and II to this Decree-Law and which are not considered essential

authorities shall notify: (a) The Commission and the Cooperation Group shall be informed of the number of essential and important entities on the list established pursuant to (3), for each of the sectors and subsectors referred to in Annex I or II; and (b) The Commission with relevant information on the number of essential and important entities identified pursuant to Article 2(2) (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service they provide and the provision, among those referred to in Article 2(2)(b) to (e) according to which they have been identified. 6. By 17 April 2025 and at the request of the Commission, Member States may notify the Commission of the names of	entities under the preceding paragraph. 3 - For the purposes of this Decree-Law, important entities are also entities of one of the types listed in Annexes I or II to this Decree-Law, referred to in Article 3(2)(b) to (e), which justify such qualification on the basis of the respective degree of exposure of the entity to risks, the size of the entity and the probability of occurrence of incidents and their severity, including their social and economic impact. 4 - The attribution of the qualifications of essential entities and important entities provided for in the

essential and important entities referred to in (5)(b).	preceding paragraphs results from the mechanisms provided for in Article 8.
Article 4º Sector-specific Union legal acts 1. Where sector-specific Union legal acts require essential and important entities to adopt cybersecurity risk-management measures or to notify significant incidents, and where those requirements are in practice at least equivalent to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement set out in Chapter VII, shall not apply to those entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall	N/A

continue to apply to entities not covered by those sector-specific Union legal acts. 2. the requirements referred to in (1) of this Article shall be considered as having equivalent effect to the obligations laid down in this Directive where: (a) The cybersecurity risk-management measures are at least equivalent in effect to those set out in Article 21(1) and (2); or (b) The sector-specific Union legal act provides for immediate, where appropriate automatic and direct access to incident notifications by CSIRTs, competent authorities or single points of contact under this Directive and where the requirements applicable to the notification of significant incidents are at least equivalent to those laid down in Article	

23(1) to (6) of this Directive. 3. The Commission shall, by 17 July 2023, provide guidance clarifying the application of (1) and (2). The Commission shall regularly review those guidelines. In developing those guidelines, the Commission shall take into account the comments of the Cooperation Group and ENISA.	
Article 5 Minimum harmonisation This Directive shall not prevent Member States from adopting or maintaining provisions ensuring a high level of cybersecurity, provided that such provisions are compatible with the obligations of Member States under Union law.	N/A
Article 6 Definitions For the purposes of this Directive,	Article 2 Definitions For the purposes of this

Draft Law No .....

the following definitions shall apply: 1) 'network and information system' means: (a) An electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972; (b) A device or group of interconnected or associated devices, one or more of which perform automatic processing of digital data on the basis of a program; or (c) Digital data stored, processed, obtained or transmitted by elements listed in points (a) and (b) for the purpose of their operation, use, protection and maintenance; 2) 'Security of network and information systems' means the	Decree-Law, the following shall mean: *a)* 'Asset' means any information and communication system, equipment and other physical and logical resources managed or owned by the entity that support, directly or indirectly, one or more services. *b)* 'Competent cybersecurity authority' means the National Cybersecurity Centre (CNCS) or, where applicable, the competent national sectoral cybersecurity authority pursuant to point (a) of Article 15(2) of this Decree-

Draft Law No .....

ability of network and information systems to withstand, at a given level of confidence, events that may jeopardise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;	Law, without prejudice to the reservations of exclusive competence of public entities with responsibilities for criminal investigation, intelligence generation and cyber defence;
3) ‘Cybersecurity’ means cybersecurity as defined in Article 2(1) of Regulation (EU) 2019/881;	*c)* Cyber threat’ means a cyber threat as defined in point 8 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;
4) ‘National cybersecurity strategy’ means a coherent framework by which a Member State defines strategic priorities and objectives in the field of cybersecurity and defines the governance with a view to achieving them in the Member State concerned;	*d)* ‘Significant cyber threat’ means a cyber threat that, based on its technical
5) ‘Near miss’ means an event that	

) could have jeopardised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems, but which could have been successfully avoided or did not materialise;	characteristics, can be considered likely to have a serious impact on the network and information systems of an entity or users of the entities' services, causing considerable material or immaterial damage;
6) 'Incident' means an event that calls into question the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems;	*e)* 'Cybersecurity' means cybersecurity as defined in point 1 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April;
7) 'Large-scale cybersecurity incident' means an incident that causes a level of disruption exceeding the response capacity of a Member State or that has a significant impact on at least two	*f)* 'Entity' means any natural or legal person created and recognised as such under the national

Draft Law No .....

Member States;	law of its place of establishment, which may, acting in its own name, exercise rights and be subject to obligations;
8) 'Incident handling' means all actions and procedures aimed at preventing, detecting, analysing, containing or responding to an incident and recovering from an incident;	*g)* 'Entities competent in the field of cyberspace security' means the Cyber Defence Command of the General Staff of the Armed Forces, the Judicial Police, the Security Intelligence Service and the Strategic Defence Intelligence Service;
9) 'Risk' means the possible loss or disruption caused by an incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of the incident occurring;	*h)* 'Entity providing domain name registration services' means a registrar or an agent acting on behalf of registrars, such as a provider or
10) 'Cyber threat' means a cyber threat as defined in Article 2(8) of Regulation (EU) 2019/881;	
11) 'Significant cyber threat' means a cyber threat that, based on its technical characteristics, can be considered likely to have a serious impact on the network	

Draft Law No .....

and information systems of an entity or users of the entities' services, causing considerable material or immaterial damage;	reseller of privacy protection or intermediary server registration services;
12) 'ICT product' means an ICT product as defined in Article 2(12) of Regulation (EU) 2019/881;	*i)* 'Technical specification' means a technical specification as defined in point 4 of Article 2 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October;
13) 'ICT service' means an ICT service as defined in Article 2. (13), of Regulation (EU) 2019/881;	*j)* 'Incident' means an event that calls into question the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via,
14) 'ICT process' means an ICT process as defined in Article 2(14) of Regulation (EU) 2019/881;	
15) 'Vulnerability' means a weakness, susceptibility or failure of an ICT product or ICT service that can be exploited by	

a cyber threat;	network and information systems;
16) 1 'Standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council;	*k)* 'Large-scale cybersecurity crisis of incident', means an incident that causes a level of disruption exceeding the capacity of the Portuguese State to respond, that has a significant impact on at least two Member States of the European Union, or that, due to its scope and systemic impact, calls for urgent intersectoral coordination;
17) 1 'Technical specification' means a technical specification as defined in Article 2(4) of Regulation (EU) No 1025/2012;	*l)* 'Significant incident' means an incident that: i) Causes, or is likely to cause, serious

Draft Law No .....

18) 'Traffic exchange point' means a network structure which allows more than two independent networks (stand-alone systems) to be interconnected, in particular in order to facilitate the exchange of internet traffic; An interchange point only interconnects autonomous systems; A peering point does not imply that internet traffic between a pair of participating autonomous systems passes through, alters or otherwise interferes with a third autonomous system;	operational disruption of services or financial losses to the entity concerned; ii) Affects or is likely to affect other natural or legal persons by causing considerable material or non-material damage. *m)* 'Risk matrix' means the reference framework establishing the risk values for the set of risk scenarios affecting a sector and subsector of activity, considering common assets, key threats and

Draft Law No .....

19) 1 'Domain name system' or 'DNS' means a hierarchically distributed name system that enables the identification of services and resources on the Internet, allowing end-user devices to use internet routing and connectivity services to access those services and resources; 20) 2 'DNS service provider' means an entity that provides: (a) Publicly available recursive domain name resolution services for internet end-users; or (b) Domain name authority resolution services for use by third parties, with the exception of root name servers;	vulnerabilities; *n)* 'Cybersecurity risk management measures or cybersecurity measures' means technical, operational and organisational measures aimed at managing the risks posed to the security of network and information systems that they use in their operations or in the provision of their services, as well as preventing or minimising the impact of incidents on recipients of their services and on other services; *o)* 'Online marketplace' means an online

Draft Law No .....

2 1) ‘Top-level domain name registry’ or ‘TLD name registry’ means an entity to which a specific TLD has been delegated and which is responsible for its administration, including the registration of domain names under the TLD and the technical operation of that TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD area files to name servers, irrespective of whether any of these operations are performed by the entity itself or are outsourced, but excluding situations where the TLD names are used by a registry for its own use only;	marketplace as referred to in Article 3(n) of Decree-Law No 57/2008 of 26 March, as amended, laying down the rules applicable to unfair commercial practices; *p)* ‘Online search engine’ means an online search engine as defined in point (5) of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June, and point (j) of Article 3 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October; *q)* ‘Standard’ means a

Draft Law No .....

2) ‘Entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a provider or reseller of privacy protection or intermediary server registration services;	standard as referred to in Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October;
	r) ‘Cybersecurity operations’ means actions to operationalise cybersecurity risk management measures;
3) ‘Digital service’ means a service as defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council;	
	s) ‘Research organisation’ means an entity whose primary purpose is to carry out applied research or experimental development with a view to exploiting the results of such research for commercial
4) ‘Trust service’ means a trust service as defined in Article 3(16) of Regulation (EU) No 910/2014;	
5) ‘Trust service provider’ means a trust service provider as defined in Article 3.(19) of Regulation (EU) No 910/2014;	

Draft Law No .....

26) ‘Qualified trust service’ means a qualified trust service as defined in Article 3(17) of Regulation (EU) No 910/2014;	purposes, excluding educational establishments;
27) ‘Qualified trust service provider’ means a qualified trust service provider as defined in Article 3(20) of Regulation (EU) No 910/2014;	*t)* ‘Social media service platform’ means an online platform, defined in accordance with point (i) of Article 3 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October, that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular through conversations, publications, videos and recommendations;
28) ‘Online marketplace’ means an online marketplace as defined in Article 2(n) of Directive 2005/29/EC of the European Parliament and of the Council;	*u)* ‘Traffic exchange
29) ‘Online search engine’ means an online search engine as defined in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council;	

Draft Law No .....

30) 'Cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and adaptable pool of shareable computing resources, including where those resources are distributed across multiple locations; 31) 'Data centre service' means a service comprising structures or groups of structures dedicated to the hosting, interconnection and centralised operation of network and IT equipment providing data storage, processing and transmission services, together with all facilities and infrastructures for energy distribution and environmental control;	point' means a network structure that: *i)* Allows the interconnection of more than two independent networks (autonomous systems), in particular in order to facilitate the exchange of Internet traffic; *ii)* Only interconnect autonomous systems; *iii)* Does not

Draft Law No .....

3 ‘Content delivery network’ 2) means a network of servers distributed geographically for the purpose of ensuring the high availability, accessibility or rapid distribution of digital content and services to internet users on behalf of content and service providers; 3 ‘Social media service platform’ 3) means a platform that enables end users to connect, share, discover and communicate with each other across multiple devices, in particular through conversations, posts, videos and recommendations;	imply that internet traffic between a pair of participating autonomous systems passes through, alters or otherwise interferes with a third autonomous system.

Draft Law No .....

3 ‘Representative’ means any 4) natural or legal person, established in the Union, expressly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, a provider of online marketplaces, online search engines or social networking service platforms that is not established in the Union, who can be contacted by a national competent authority or a CSIRT, instead of the entity represented, in relation to the latter’s obligations under this Directive;	

Draft Law No .....

3 5) ‘Government entity’ means an entity, recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, that meets the following criteria: (a) It is established for the purpose of meeting needs in the general interest and is not of an industrial or commercial character; (b) Has legal personality or is empowered by law to act on behalf of another entity having legal personality; (c) It is financed, for the most part, by the State, regional authorities or other bodies governed by public law; its management is subject to supervision by those authorities or bodies; or more than half the members of its administrative, managerial or	

Draft Law No .....

36) 3 'Public electronic communications network' means a public electronic communications network as defined in Article 2(8) of Directive (EU) 2018/1972;	
37) 3 'Electronic communications service' means an electronic communications service as defined in Article 2(4) of Directive (EU) 2018/1972;	
38) 3 'Entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting in its own name, exercise rights and be subject to obligations;	

Draft Law No .....

39) ‘Managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructures, applications or any other network and information systems, through active on-site or off-site assistance or administration; 40) ‘Managed security service provider’ means a managed service provider that performs or provides assistance for activities related to cybersecurity risk management;	

Draft Law No .....

4 'Research organisation' means 1) an entity whose primary purpose is to carry out applied research or experimental development with a view to exploiting the results of such research for commercial purposes, excluding educational establishments.	
	v) 'DNS service provider' means an entity that provides publicly available recursive domain name resolution services for internet end-users or resolution services with authority for domain names for use by third parties, with the exception of root name servers; *w)* 'Trust service provider' means a trust service

	provider as defined in point 19 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April; *x)* 'Managed security service provider' means a managed service provider that performs or provides assistance for activities related to cybersecurity risk management;

	y) 'Managed service provider' means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructures, applications or any other network and information systems, through assistance or active administration performed at customer premises or remotely; *z)* 'Qualified trust service provider' means a qualified trust service provider as referred to in point 20 of Article 3 of Regulation (EU) No

Draft Law No .....

	910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April; *aa)* 'ICT process' means an ICT process as defined in point 14 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April; *bb)* 'ICT product' means an ICT product as defined in

Draft Law No .....

	point (12) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April; *cc)* 'Near miss' means an event that could have jeopardised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems, but which could have been successfully avoided or did not materialise; *dd)* 'Content delivery network' means a

Draft Law No .....

	network of servers distributed geographically for the purpose of ensuring the high availability, accessibility or rapid distribution of digital content and services to internet users on behalf of content and service providers; *ee)* 'Registration of top-level domain names' or 'Registration of TLD (Top Level Domain)' names means an entity to which a specific TLD has been delegated and which is responsible for its administration, including the registration of domain names under

	the TLD and the technical operation of that TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files to name servers, irrespective of whether any of these operations are performed by the entity itself or are outsourced, but excluding situations where the names of the TLD are used by a registry for its own use only; *ff)* 'Public electronic communications network' means a public electronic communications network within the

Draft Law No .....

	meaning of point (oo) of Article 3(1) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended; *gg)* 'Networks and information systems' means: *i)* An electronic communications network, pursuant to point (mm) of Article 3(1) of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended; *ii)* A device or group of

Draft Law No .....

	interconnected or associated devices, one or more of which perform automatic processing of digital data on the basis of a program; or *iii)* Digital data stored, processed, obtained or transmitted by elements referred to in points (i) and (ii) for the purpose of their operation, use, protection and maintenance; *hh)* 'Representative' means any natural or legal person,

	established in the European Union, expressly designated to act on behalf of a DNS service provider, a Top Level Domain Name Registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, a provider of online marketplaces, online search engines or social media service platforms that is not established in the European Union,

Draft Law No .....

	who can be contacted by the competent entities, instead of the entity represented, in relation to the latter's obligations under this Decree-Law; *ii)* 'Risk' means the possible loss or disruption caused by an incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of the incident occurring; *jj)* 'Residual risk' means a risk measure that exists after the adoption of the minimum cybersecurity

Draft Law No .....

	measures; *kk)* 'Security of network and information systems' means the ability of network and information systems to withstand, at a given level of confidence, events that may jeopardise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those networks and information systems; *ll)* 'Data centre service' means a service comprising structures or groups

	of structures dedicated to the hosting, interconnection and centralised operation of network and IT equipment providing data storage, processing and transmission services, together with all facilities and infrastructures for energy distribution and environmental control; *mm)* 'Cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and adaptable pool of shareable computing resources, including where those

Draft Law No .....

	resources are distributed across multiple locations; *nn)* 'Electronic communications service' means an electronic communications service pursuant to point (ss) of Article 3 of the Electronic Communications Law, approved by Law No 16/2022 of 16 August, as amended; *oo)* 'Trust service' means a trust service as defined in point 16 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU)

Draft Law No .....

	2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April;
	pp) 'Qualified trust service' means a qualified trust service as defined in Article 3(17) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July, as amended by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and Regulation (EU) No 2024/1183 of the European Parliament

	and of the Council of 11 April; *qq)* 'ICT service' means an ICT service as defined in point (13) of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April; *rr)* 'Domain name system' or 'DNS' means a hierarchically distributed name system that enables the identification of services and resources on the Internet, allowing end-user devices to use internet routing and connectivity services to access those services and

	resources; *ss)* 'Digital service' means a service within the meaning of Article 3(g) of Decree-Law No 30/2020 of 29 June laying down the rules governing the information procedure in the field of technical rules on products and rules on information society services; *tt)* 'Incident handling' means all actions and procedures aimed at preventing, detecting, analysing, containing or responding to an incident and recovering from an incident;

Draft Law No .....

	uu) 'Vulnerability' means a fragility, susceptibility or failure, affecting network and information systems, information or communication technology (ICT) products or services, that can be exploited by a cyber threat.
Article 7 National Cybersecurity Strategy 1. Each Member State shall adopt a national cybersecurity strategy setting out the strategic objectives, the resources needed to achieve those objectives and the appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:	Article 12 National Cybersecurity Strategy 6 - The National Cyberspace Security Strategy (ENSC) defines the framework, priorities, national strategic objectives and a governance framework defining the roles and responsibilities of

(a) The objectives and priorities of the cybersecurity strategy of the Member State, covering in particular the sectors referred to in Annexes I and II; (b) A governance framework to meet the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in (2);	stakeholders at national level relevant to the implementation of the ENSC. 7 - ENCS includes, *inter alia*: k) The objectives and priorities of the ENCS, covering, in particular, the sectors in Annexes I and II to this Decree-Law; l) A governance framework to meet the objectives and priorities referred to in point (a) of this paragraph; m) A governance framework defining the roles and responsibilities of stakeholders at national level relevant to the

Draft Law No .....

(cA governance framework) clarifying the roles and responsibilities of relevant stakeholders at national level, consolidating cooperation and coordination at national level between competent authorities, single points of contact and CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts; (dA mechanism to identify relevant) assets and a risk assessment in that Member State; (eIdentification of preparedness,) response, and recovery measures in case of incidents, including public-private cooperation;	implementation of the ENSC and consolidating institutional cooperation and coordination under this Decree-Law; n) A mechanism to identify relevant assets and a risk assessment in Portugal; o) Identification of preparedness, response, and recovery measures in case of incidents, including public-private cooperation; p) A list of the various authorities and stakeholders involved in the implementation of the ENCS; q) A policy framework

Draft Law No .....

(f) A list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy; (g) A policy framework for enhanced cooperation between competent authorities under this Directive and competent authorities under Directive (EU) 2022/2557 for the purpose of sharing information on risks, cyber threats, and incidents, as well as non-cyber risks, threats and incidents, and exercising supervisory tasks as appropriate; (h) A plan, including the necessary measures, to increase the general level of cybersecurity awareness of citizens. 2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:	for enhanced cooperation between competent authorities pursuant to this Decree-Law and competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December for the purposes of information sharing on risks, cyber threats and incidents, as well as non-cyber risks, threats and incidents, and the exercise of supervisory tasks; r) A plan, including the necessary measures, to enhance the

Draft Law No .....

(a) On cybersecurity in the supply chain of ICT products and ICT services used by entities in the provision of their services; (b) On the inclusion and specification of cybersecurity requirements for ICT products and ICT services in public procurement procedures, including as regards cybersecurity certification, encryption and the use of open-source cybersecurity products; (c) Ensuring vulnerability management, including promoting and facilitating coordinated vulnerability disclosure in accordance with Article 12(1).	general level of education, training and awareness of citizens on cybersecurity and cyber hygiene; s) A plan, including the necessary measures, appropriate to the specific cybersecurity needs of small and medium-sized enterprises, qualified in accordance with Article 2 of Annex III to this Decree-Law, corresponding to those of Commission Recommendation 2003/361/EC of 6 May; t) Promoting the development, research and integration of

Draft Law No .....

(d) On maintaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables; (e) Promote the development and integration of relevant advanced technologies aimed at implementing state-of-the-art cybersecurity risk management measures; (f) Promote and develop cybersecurity education and training, cybersecurity skills, awareness-raising and research and development initiatives in the field of cybersecurity, as well as guidance on good practices and cyber hygiene controls, for citizens, stakeholders and entities;	advanced technologies for the implementation of innovative measures, best practices and controls, including the use of artificial intelligence, in cybersecurity risk management and in the detection and prevention of cyber-attacks. 8 - The ENSC is approved by resolution of the Council of Ministers, on a proposal from the National Cybersecurity Centre (CNCS), after hearing the Superior Council for Cyberspace Security (CSSC), after a period of public consultation of no less than 30 days. 9 - The ENCS is

Draft Law No .....

(g) Support academic and research institutions in developing, improving and promoting the deployment of cybersecurity tools and secure network infrastructures; (h) Include relevant procedures and appropriate information sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law; (i) Strengthen the cyber resilience and cyber hygiene baseline of small and medium-sized enterprises, especially those excluded from the scope of this Directive, by providing easily accessible guidance and assistance tailored to their specific needs;	reviewed and updated every five years, following an evaluation process based on key impact and performance indicators, and this period may be reduced by decision of the member of the Government responsible for cybersecurity upon a reasoned proposal from the CNCS. 10 - The ENSC shall be without prejudice to the approval by the competent authorities, where necessary, of instruments establishing sectoral cybersecurity strategies, which shall be reviewed and updated in the same terms as those applicable to the ENSC.

Draft Law No .....

(j Promoting active cyber) protection. 3. Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information related to their national security from such notifications. 4. Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. At the request of Member States, ENISA shall assist them in formulating or updating the national cybersecurity strategy and key performance indicators for the evaluation of that strategy in order to align it with the requirements and obligations set out in this Directive.	

Draft Law No .....

Article 8 Competent authorities and single points of contact 1. Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for carrying out the supervisory tasks set out in Chapter VII (competent authorities). 2. The competent authorities referred to in (1) shall monitor the implementation of this Directive at national level. 3. Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to (1), this is also the single point of contact of that Member State. 4. Each single point of contact shall have a liaison function to ensure cross-border cooperation of the authorities of its Member State with the competent authorities of	Article 15 Organisation 1 - The institutional framework for cyberspace security shall be composed of the following entities: a) The CSSC, as an advisory body to the Prime Minister in the field of cybersecurity; b) The CNCS, in its capacity as: i) National Cybersecurity Authority; ii) single point of contact for the purposes of cooperation within the European

other Member States and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities of its Member State. 5. Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out their tasks effectively and efficiently and thereby fulfil the objectives of this Directive. 6. Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in (1) and of the single point of contact referred to in (3), their respective functions and any subsequent changes thereto. Each Member State shall publish the identity of its competent authority. The Commission shall publish a list of single points of contact.	Union and at international level, without prejudice to the competences conferred on other entities in the field of international criminal cooperation; iii) National Cybersecurity Certification Authority; iv) Member of the National Cybersecurity Incident Response Team. c) The Secretary-General of the Internal Security System, in his

Draft Law No .....

	capacity as the national authority for managing large-scale cybersecurity incidents and crises. 2 - They are also part of the coordinated cybersecurity framework: a) As sectoral national cybersecurity authorities: i) the National Security Office (NSO) with regard to trust services in electronic transactions in the internal

Draft Law No .....

	market; ii) The National Communications Authority (ANACOM), with regard to electronic communications and the postal service. b) As special national cybersecurity authorities, with regard to the matter of digital operational resilience of the financial sector: i) The Supervisory Authority for Insurance and Pension Funds (ASF);

Draft Law No .....

	ii) The Securities Market Commission (CMVM); iii) The Bank of Portugal. c) The Cyber Security Assessment Commission. d) The Judicial Police; e) The Security Intelligence Service; f) The Strategic Defence Intelligence Service; g) The Cyber Defence Operations Command. 3 - The organisation

	of the institutional framework for cyberspace security shall be without prejudice to the informal coordination of the authorities referred to in this Article, including through participation in multilateral coordination fora concerning the defence of cyberspace security, such as the Cyberspace Liaison Officers Office for tactical-operational cooperation (G5). Article 19 National Cybersecurity Centre 1 - The National Cybersecurity Centre (CNCS) is the national cybersecurity authority,

Draft Law No .....

	whose mission is to ensure that the country achieves and maintains a high level of cybersecurity, through the promotion of continuous improvement of national cybersecurity and international cooperation, as well as the definition and implementation of the measures and instruments necessary for the anticipation, detection, reaction and recovery of situations that, in the face of the imminence or occurrence of incidents, jeopardise the national interest, the functioning of essential entities, important entities and relevant public entities. 2 - The CNCS is also the single point of contact for the purposes of cooperation at the

Draft Law No .....

	European Union level, as well as at the international level on cybersecurity, without prejudice to the powers conferred on other authorities with regard to cooperation in criminal matters, in particular the powers of the Criminal Police for international cooperation conferred on it by Articles 20 to 26 and Article 29 of the Cybercrime Law, and with regard to the production of information relating to the internal and external security of the Portuguese State and its allies. 3 - The CNCS is part of the 'CERT.PT', provided for in Article 22, which acts as the National Cybersecurity Incident Response Team.

Draft Law No .....

	4 - The CNCS is also the national cybersecurity certification authority, in particular for the purposes of Article 58 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April, without prejudice to the competences of the GNS as regards the certification and accreditation of information and communication systems processing classified information, pursuant to Decree-Law No 3/2012 of 16 January, as amended.
Article 9º National cyber crisis management frameworks	Article 13 National Plan for Responding to Large-Scale Cybersecurity

Draft Law No .....

1. Member States shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber-crisis management authorities). Member States shall ensure that those authorities have the necessary resources to carry out their tasks effectively and efficiently. Member States shall ensure consistency with existing general crisis management frameworks at national level. 2. Where a Member State designates or establishes more than one cyber crisis management authority referred to in (1), it shall clearly indicate which of those authorities is to act as coordinator for the management of large-scale cybersecurity incidents and crises. 3. Each Member State shall identify capabilities, assets and procedures that can be used in the event of a crisis for the purposes of	Crises and Incidents 1 - The National Plan for Response to Large-Scale Cybersecurity Incidents and Crises sets out the objectives and modalities for the management of such large-scale cybersecurity incidents and crises. 2 - The national plan for responding to large-scale cybersecurity crises and incidents shall be approved by a resolution of the Council of Ministers, on a joint proposal from the Secretary-General of the Internal Security System, the Criminal Police, the Security Intelligence Service, the Strategic Defence Information Service,

this Directive. 4. Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan setting out the objectives and arrangements for managing large-scale cybersecurity incidents and crises. That plan shall set out, in particular: (a) The objectives of national preparedness activities and measures; (b) The roles and responsibilities of cyber crisis management authorities; (c) Cyber crisis management procedures, including their integration into the overall crisis management framework and information exchange channels;	the Cyber Defence Operations Command and the CNCS, the latter being responsible for its implementation, follow-up and monitoring, in close cooperation with the entities making up the crisis office provided for in Article 16(4) of Law 53/2008 of 29 August, as amended by this Decree-Law, and after consulting the CSSC. 3 - The national large-scale cybersecurity incident and crisis response plan shall ensure consistency with existing general crisis management frameworks at national level.

Draft Law No .....

(d) National preparedness measures, including exercises and training activities; (e) The relevant public and private stakeholders and infrastructure involved; (f) National procedures and arrangements between the relevant national authorities and bodies to ensure the Member State's support for and effective participation in the coordinated management of large-scale cybersecurity incidents and crises at Union level. 5. Within three months of the designation or establishment of the Cyber Crisis Management Authority referred to in (1), each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and	Article 21 Cybersecurity Crisis Management Authority 1 - The Secretary-General of the Internal Security System is the national authority for managing large-scale cybersecurity incidents and crises, also referred to as the cybersecurity crisis management authority. 2 - The declaration of large-scale cybersecurity incidents and crises depends on the attribution of a 'high' threat level by the Security Intelligence Service, in accordance with the Plan for the coordination, control and operational

the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) relevant information on the requirements of (4) on their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information to the extent that such exclusion is necessary to safeguard their national security.	command of the Security Forces and Services, approved by Council of Ministers Decision No DB 14/2010 of 5 March, or on the communication by the CNCS of the occurrence of a large-scale cybersecurity incident or crisis, in accordance with Article 20(1)(g). 3 - The Secretary-General of the Internal Security System shall convene the Cybersecurity Crisis Office, pursuant to Article 16(4) of Law No 53/2008 of 29 August, as amended,
Article 10 Computer Security Incident Response Teams (CSIRTs)	Article 22 Cybersecurity Incident

Draft Law No .....

1. Each Member State shall designate or establish one or more CSIRTs. CSIRTs may be designated or established within a competent authority. CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entities referred to in Annexes I and II, and shall be responsible for incident handling according to a well-defined process. 2. Member States shall ensure that each CSIRT has adequate resources to effectively perform its tasks as set out in Article 11(3). 3. Member States shall ensure that each CSIRT has at its disposal an adequate, secure and resilient information and communication infrastructure through which it can exchange information with essential and important entities and other stakeholders. To this end, they shall ensure that each CSIRT contributes to the	Response Team 1 - 'CERT.PT' is the national cybersecurity incident response team. 2 - 'CERT.PT' is integrated into the CNCS and has technical and operational autonomy. 3 - 'CERT.PT' shall exercise the following competences: a) Ensure operational incident response; b) Monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, assisting relevant

deployment of secure information sharing tools. 4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29, with sectoral or cross-sectoral communities of essential and important entities. 5. CSIRTs shall participate in peer reviews organised pursuant to Article 19. 6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs within the CSIRTs network. 7. CSIRTs may establish cooperative relations with national computer security incident response teams from third countries. Within the framework of those cooperation relations, Member States shall facilitate an effective, efficient and secure exchange of information with those third country national computer security incident response teams,	essential, important and public entities with real-time or near-real-time monitoring of their networked systems and information; c) Activate early warning mechanisms, send alert messages, communicate and disseminate information to relevant essential, important and public entities, competent authorities, and other stakeholders, on cyber threats, vulnerabilities and incidents, including in real

using relevant information sharing protocols, including the Light Signalling Protocol. CSIRTs may exchange relevant information with national computer security incident response teams of third countries, including personal data, in accordance with Union data protection law. 8. CSIRTs may cooperate with national computer security incident response teams of third countries or equivalent bodies of third countries, including to provide them with cybersecurity assistance. 9. Each Member State shall notify the identity of the CSIRT referred to in (1) of this Article to the Commission without undue delay, and of the coordinating CSIRT designated in accordance with Article 12(1), their functions in relation to essential and important entities and any subsequent changes thereto. 10. Member States may request	time; d) Intervene in the event of incidents and provide assistance to relevant essential, important, and public entities, including, where applicable, by proposing to the CNCS the issuance of operational orders, instructions, and guidelines on measures to be taken to contain, mitigate, and resolve incidents, as well as appropriate deadlines for their implementation; e) In situations of

the assistance of ENISA in setting up their CSIRTs.	proven serious risk, propose to the competent cybersecurity authority the adoption of implementing measures necessary for an immediate response to the cyber threat, incident or crisis, in accordance with Article 52(3), where the relevant essential, important or public entity concerned does not do so on a voluntary basis; f) Collect and analyse forensic data, determine its preservation, perform dynamic

	risk and incident analysis, and develop cybersecurity situational awareness; g) Carry out, at the request of a relevant essential, important or public entity, a proactive analysis of the entity's respective network and information systems in order to detect vulnerabilities with a potential significant impact; h) Implement tools and functionalities that enable the secure sharing of information with

	essential, important, and relevant public entities, as well as with other stakeholders; i) Carry out, on its own initiative, proactive and non-intrusive analyses of publicly accessible network and information systems of relevant essential, important and public entities, with the aim of detecting vulnerable or unsafe network and information systems and informing the entities concerned, insofar as they do not

Draft Law No .....

	have any negative impact on the functioning of their services; j) Promote the adoption and use of common or standardised practices; k) Ensure national representation in the network of national cybersecurity incident response teams pursuant to Article 20(1)(l)(ii) and other international forums for cooperation of cybersecurity incident response teams; l) Participate in national forums

Draft Law No .....

	for cooperation of Computer Security Incident Response Teams; m) Participate in national and international events and training sessions; n) Collaborate and coordinate with sectoral, national and European CSIRTs networks, whenever necessary or appropriate. o) Cooperate with the competent entities in the field of cyberspace security. 4 - In the exercise of its powers, 'CERT.PT' may determine the

	prioritisation of certain tasks through a risk-based approach, taking into account, *inter alia*, the existing threat assessment produced by the Security Intelligence Service. 5 - Public and private entities shall cooperate with 'CERT.PT' in the exercise of their respective tasks and powers under this Decree-Law. 6 - The collaboration referred to in the previous paragraph may include physical access to facilities and information sharing between entities providing

Draft Law No .....

	incident response services to third parties and 'CERT.PT', and joint actions, at its initiative, for the purposes of (3)(e).
Article 11 Requirements, technical capabilities and functions of CSIRTs 1. CSIRTs shall comply with the following requirements:	Article 22 Cybersecurity Incident Response Team 1 - 'CERT.PT' is the national cybersecurity incident response team. 2 - 'CERT.PT' is integrated into the CNCS and has technical and operational autonomy. 3 - 'CERT.PT' shall exercise the following

Draft Law No .....

(a) CSIRTs should ensure wide availability of their communication channels, avoiding one-off failures, and should have various means to contact other parties and to be contacted at any time. CSIRTs shall clearly specify the communication channels and disseminate them to their customer base and cooperation partners; (b) CSIRTs facilities and their supporting information systems shall be located in secure locations; (c) CSIRTs shall be equipped with an appropriate request management and routing system, in particular to facilitate effective and efficient transfers;	competences: a) Ensure operational incident response; b) Monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, assisting relevant essential, important and public entities with real-time or near-real-time monitoring of their networked systems and information; c) Activate early warning mechanisms, send alert messages, communicate and disseminate

(d) CSIRTs shall ensure the confidentiality and credibility of their operations; (e) CSIRTs shall have sufficient staff to ensure the availability of their services at all times and shall ensure that their staff is adequately trained; (f) CSIRTs shall be equipped with redundant systems and have a fallback workspace to ensure continuity of their services. CSIRTs may participate in international cooperation networks. 2. Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to perform the tasks referred to in (3). Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop	information to relevant essential, important and public entities, competent authorities, and other stakeholders, on cyber threats, vulnerabilities and incidents, including in real time; d) Intervene in the event of incidents and provide assistance to relevant essential, important, and public entities, including, where applicable, by proposing to the CNCS the issuance of operational orders,

their technical capabilities. 3. The tasks of the CSIRTs shall be the following: (a) Monitor and analyse cyber threats, vulnerabilities and incidents at national level and, upon request, assist essential and important entities concerned with real-time or near-real-time monitoring of their network and information systems; (b) Activate early warning mechanisms, send alert messages, communicate and disseminate information to essential and important entities, as well as competent authorities and other stakeholders, on cyber threats, vulnerabilities and incidents, where possible in near real-time;	instructions, and guidelines on measures to be taken to contain, mitigate, and resolve incidents, as well as appropriate deadlines for their implementation; e) In situations of proven serious risk, propose to the competent cybersecurity authority the adoption of implementing measures necessary for an immediate response to the cyber threat, incident or crisis, in accordance with Article 52(3), where the relevant

Draft Law No .....

(c) Intervene in the event of incidents and provide assistance to the essential and important entities involved, where applicable;	essential, important or public entity concerned does not do so on a voluntary basis;
(d) Collect and analyse forensic data, perform dynamic risk and incident analysis and develop cybersecurity situational awareness;	f) Collect and analyse forensic data, determine its preservation, perform dynamic risk and incident analysis, and develop cybersecurity situational awareness;
(e) Carry out, at the request of an essential or important entity, a proactive analysis of the network and information systems of the entity concerned in order to detect vulnerabilities with a potential significant impact;	g) Carry out, at the request of a relevant essential, important or public entity, a proactive analysis of the entity's respective network and

(f) Participate in the CSIRTs network and provide mutual assistance, in accordance with their capabilities and competences, to other members of the CSIRTs network upon their request;	information systems in order to detect vulnerabilities with a potential significant impact;
(g) Where applicable, act as coordinator for the coordinated vulnerability disclosure process referred to in Article 12(1);	h) Implement tools and functionalities that enable the secure sharing of information with essential, important, and relevant public entities, as well as with other stakeholders;
(h) Contribute to the deployment of secure information sharing tools pursuant to Article 10(3).	
CSIRTs may perform a proactive and non-intrusive analysis of publicly accessible network and information systems of essential and important entities. That analysis shall be carried out with the aim of detecting vulnerable or unsafe network and information systems and of informing the entities concerned. Such analysis	i) Carry out, on its own initiative, proactive and non-intrusive analyses of publicly accessible network and information systems of relevant essential,

should not have any negative impact on the functioning of the entities' services. When carrying out the tasks referred to in the first subparagraph, CSIRTs may prioritise certain tasks on the basis of a risk-based approach. 4. CSIRTs shall establish cooperative relationships with relevant private sector stakeholders with a view to best achieving the objectives of this Directive. 5. In order to facilitate the cooperation referred to in (4), CSIRTs shall promote the adoption and use of common or standardised practices, classification systems and taxonomies in relation to: (a) Incident handling procedures; (b) Crisis management; and	important and public entities, with the aim of detecting vulnerable or unsafe network and information systems and informing the entities concerned, insofar as they do not have any negative impact on the functioning of their services; j) Promote the adoption and use of common or standardised practices; k) Ensure national representation in the network of national cybersecurity

(c) Coordinated vulnerability disclosure in accordance with Article 12(1).	incident response teams pursuant to Article 20(1)(l)(ii) and other international forums for cooperation of cybersecurity incident response teams; l) Participate in national forums for cooperation of Computer Security Incident Response Teams; m) Participate in national and international events and training sessions; n) Collaborate and coordinate with sectoral, national and European CSIRTs networks,

Draft Law No .....

	whenever necessary or appropriate. o) Cooperate with the competent entities in the field of cyberspace security. 4 - In the exercise of its powers, 'CERT.PT' may determine the prioritisation of certain tasks through a risk-based approach, taking into account, *inter alia*, the existing threat assessment produced by the Security Intelligence Service. 5 - Public and private entities shall cooperate with 'CERT.PT' in the

Draft Law No .....

	exercise of their respective tasks and powers under this Decree-Law. 6 - The collaboration referred to in the previous paragraph may include physical access to facilities and information sharing between entities providing incident response services to third parties and 'CERT.PT', and joint actions, at its initiative, for the purposes of (3)(e).
Article 12 Coordinated vulnerability disclosure and European vulnerability database 1. Each Member State shall designate one of its CSIRTs as a	Article 38 Vulnerabilities in information systems 1 - 'CERT.PT' is the national coordinating entity for the

coordinator for coordinated vulnerability disclosure. The CSIRT designated as coordinator shall perform the role of trusted intermediary, facilitating, where necessary, the interaction between the notifying natural or legal person and the manufacturer or provider of potentially vulnerable ICT products or ICT services, at the request of either party. The tasks of the CSIRT designated as coordinator shall include: (a) The identification and contact details of the entities concerned; (b) Providing support to natural or legal persons reporting vulnerabilities; and (c) Negotiating the disclosure schedule and managing vulnerabilities affecting multiple entities. Member States shall ensure that	coordinated disclosure of vulnerabilities affecting information and communication technology networks and systems, products, components and services. 2 - 'CERT.PT' shall act as a trusted intermediary, facilitating, where necessary, the interaction between the notifying natural or legal person and the manufacturer or provider of potentially vulnerable ICT products or ICT services, at the request of either party. 3 - The tasks of 'CERT.PT' shall include, in particular: a) The identification and contact details

natural or legal persons can report a vulnerability to the designated coordinator CSIRT on an anonymous basis if they so request. The CSIRT designated as coordinator shall ensure that diligent follow-up actions are carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. In cases where the notified vulnerability may have a material impact on entities in more than one Member State, the CSIRT designated as coordinator by each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network. 2. After consulting the Cooperation Group, ENISA shall establish and maintain a European vulnerability database. To that end, it shall establish and maintain appropriate information systems,	of the entities referred to in the preceding paragraph; b) Providing support to natural or legal persons reporting vulnerabilities; c) Negotiating the disclosure schedule and managing vulnerabilities affecting multiple entities. 4 - 'CERT.PT' shall preserve the anonymity of any natural or legal person who has reported a vulnerability, should that person so request, without prejudice to the provisions of the Cybercrime Law, approved by Law No 109/2009 of 15

policies and procedures, and adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view, in particular, to enabling entities, irrespective of whether they fall within the scope of this Directive, and their network and information system providers, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders should have access to the vulnerability information contained in the European Vulnerability Database. That database shall include: (a) Information describing the vulnerability;	September, as amended by this Decree-Law. 5 - The data included in the communications made under this Article shall be deleted within 10 days from the moment the vulnerability is rectified, and their confidentiality shall be guaranteed throughout the procedure. Article 39 Vulnerability reporting Where vulnerability may have a major impact on entities in more than one Member State of the European Union, 'CERT.PT' cooperates with its counterparts, either within the European Network of CSIRTs or within the EU-CyCLONe framework.

(b) The affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it can be exploited; (c) The availability of patches and, in the absence of patches, guidance provided by competent authorities or CSIRTs to users of vulnerable ICT products and ICT services on how to minimise the risks resulting from the disclosed vulnerabilities.	
Article 13 Cooperation at national level 1. Where the competent authorities, the single point of contact and the CSIRTs of the same Member State are separate entities, they shall cooperate with each other with regard to compliance with the obligations laid down in this Directive. 2. Member States shall ensure	Article 23 Cooperation between national authorities 1 - The CNCS, the Secretary-General of the Internal Security System, and the national sectoral cybersecurity authorities, in the exercise of their tasks and powers

that their CSIRTs or, where applicable, their competent authorities receive notifications of significant incidents in accordance with Article 23, and on incidents, cyber threats and near misses, pursuant to Article 30. 3. Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single point of contact of notifications of incidents, cyber threats and near misses made pursuant to this Directive. 4. In order to ensure that the tasks and obligations of competent authorities, single points of contact and CSIRTs are carried out effectively, Member States should ensure, to the extent possible, appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, national authorities pursuant to Regulations (EC)	under this Decree-Law, shall act in close cooperation with: a) The National Data Protection Commission, whenever incidents giving rise to a personal data breach are concerned, in accordance with Article 79; b) The Public Prosecutor's Office, the courts, and the Judicial Police, whenever incidents are involved that may have led to the commission of cybercrimes, namely through: i) the

No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, competent authorities years under Regulation (EU) 2022/2554, national regulatory authorities under Directive (EU) 2018/1972, competent authorities under Directive (EU) 2022/2557, as well as competent authorities under other sector-specific Union legal acts within that Member State. 5. Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and regularly exchange information on the identification of critical entities, on risks, cyber threats and incidents, as well as on non-cyber risks, threats and incidents affecting essential entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to those risks, threats		communication, as soon as possible, of facts relating to the preparation and execution of cybercrimes of which they have become aware in the exercise of their functions, without prejudice to the provisions of Article 38 of this Decree-Law; ii) The practice of

and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats. 6. Member States shall simplify the communication of information through technical means for the notifications referred to in Articles 23 and 30.		the necessary and urgent precautionary acts to ensure the preservation of evidence and the sharing, in legal terms, of other evidence necessary for the strict exercise of the powers provided for in (3)(a) to (e) of the preceding Article; iii) the performance of the

Draft Law No .....

	function of expert provided for in Article 153 of the Code of Criminal Procedure. c) The Cyber Defence Operations Command, namely when it concerns incident prevention, monitoring, detection, reaction, analysis, and correction in the context of cyber defence and cyber security of the Armed Forces; d) The Security

Draft Law No .....

	Intelligence Service, in particular in the sharing of information necessary for the preservation of the security of cyberspace of national interest, in particular as regards espionage, sabotage, terrorism and organised crime. 2 - Obtaining information under the cooperation provided for in the preceding paragraph must comply with the applicable legislation on the protection of personal data, namely the GDPR,

Draft Law No .....

	Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8 August, and Law No 59/2019 of 8 August. 3 - The cooperation provided for in point (b) of paragraph 1 shall not jeopardise the confidentiality of judicial proceedings. 4 - Access to information in accordance with the cooperation provided for, in particular, in (1)(b)(i) and (ii), relating to cases under investigation, may be refused on the grounds provided for in Article 89(1) of the Code of Criminal Procedure.

Draft Law No .....

	5 - The Judiciary Police and the Security Intelligence Service shall designate a permanent liaison officer to the CNCS. 6 - The terms of technical and operational cooperation between the CNCS, the Cyber Defence Operations Command, the Criminal Police, the Security Intelligence Service and the Strategic Defence Intelligence Service are defined by mutual agreement within the G5. 7 - The authorities referred to in this Article shall reply to requests for

	information within five days of the date on which the information was requested, unless there are duly justified grounds.
Article 14 Cooperation Group 1. A Cooperation Group shall be established to support and facilitate strategic cooperation and information exchange between Member States, as well as to build trust. 2. The Cooperation Group shall perform its tasks on the basis of the biennial work programmes referred to in (7). 3. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA. The European External Action Service shall participate in	N/A

the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that regulation. Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work. The secretariat of the group shall be provided by the Commission. 4. The tasks of the Cooperation Group shall be: (a) Provide guidance to competent authorities on the transposition and application of this Directive;	

(b) Provide guidance to competent authorities on the development and implementation of coordinated vulnerability disclosure policies as referred to in Article 7(2)(c);	
(c) Exchanging best practices and information on the implementation of this Directive, including on cyber threats, incidents, vulnerabilities, near misses, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications, as well as the identification of essential and important entities in accordance with Article 2(2)(b) to (e);	

Draft Law No .....

	(d) Exchanging opinions and cooperating with the Commission on new policy initiatives in the area of cybersecurity and the overall coherence of sectoral cybersecurity requirements;	
Carry out coordinated security risk assessments of critical supply chains in accordance with Article	(e) Exchanging opinions and cooperating with the Commission on draft delegated or implementing acts adopted pursuant to this Directive;	
Discuss cases of mutual assistance, including experiences and results of cross-border joint supervisory actions as referred to	(f) Exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;	
At the request of one or more Member States concerned, discuss specific requests for mutual assistance referred to in	(g) Hold exchanges of views on the implementation of sector-specific Union legal acts containing provisions on cybersecurity;	

(l) Provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;	
(m) Exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises, based on lessons learned from the CSIRTs network and EU-CyCLONe;	
(n) Contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials as part of a capability development programme or staff of competent authorities or CSIRTs;	

Draft Law No .....

(o) Organise regular joint meetings with private stakeholders from across the Union to discuss the activities of the Cooperation Group and share views on new policy challenges; (p) Discuss the work carried out in relation to cybersecurity exercises, including the work carried out by ENISA;	

(q) Establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1) and establish the self-assessment methodology for Member States pursuant to Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, draw up codes of conduct underpinning the working methods of cybersecurity experts designated in accordance with Article 19(6);	
(r) For the purposes of the assessment referred to in Article 40, prepare reports on experience gained at strategic level and through peer reviews;	
(s) Discuss and regularly carry out an assessment of the state of play of cyber threats or incidents, such as ransomware.	
The Cooperation Group shall	

submit the reports referred to in point (r) of the first subparagraph to the Commission, the European Parliament and the Council. 5. Member States shall ensure the effective, efficient and secure cooperation of their representatives in the Cooperation Group. 6. The Cooperation Group may request from the CSIRTs Network a technical report on certain topics. 7. By 1 February 2024, and every two years thereafter, the Cooperation Group shall draw up a work programme for the actions to be undertaken to achieve its objectives and carry out its tasks. 8. The Commission may adopt implementing acts laying down the procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to	

in Article 39(2). The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4)(e). 9. The Cooperation Group shall meet regularly, and in any event at least once a year, with the Critical Entities Resilience Group established pursuant to Directive (EU) 2022/2557, with a view to promoting and facilitating strategic cooperation and information exchange.	
Article 15 CSIRTs Network 1. A network of national CSIRTs shall be established to contribute to the development of trust and promote swift and effective operational cooperation between	Article 39 Vulnerability reporting Where the vulnerability has a major impact on entities in more than one Member State of the European Union, 'CERT.PT' cooperates with its

Member States. 2. The CSIRTs network shall be composed of representatives of the CSIRTs designated or established in accordance with Article 10 and the Computer Emergency Response Team for the Union institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA provides secretarial services and actively supports cooperation between CSIRTs. 3. The functions of the CSIRTs network shall be the following: (a) Exchange information on the capabilities of CSIRTs; (b) Facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among CSIRTs;	counterparts, either within the European Network of CSIRTs or within the EU-CyCLONe framework.

(c) Exchange important information on incidents, near misses, cyber threats, risks and vulnerabilities;	
(d) Exchange information on cybersecurity publications and recommendations;	
(e) Ensure interoperability with regard to information sharing specifications and protocols;	
(f) At the request of a member of the CSIRTs network potentially affected by an incident, exchange and discuss information related to those incidents and related cyber threats, risks and vulnerabilities;	

Draft Law No .....

(j) Discuss and identify other forms of operational cooperation, in particular with regard to: (i) Categories of cyber threats and incidents; ii) Early warnings; iii) Mutual assistance, iv) Principles and forms of coordination in responding to risks and incidents with a cross-border dimension; v) The contribution to the national response plan for large-scale cybersecurity incidents and crises referred to in Article 9(4), at the request of a Member State;	

Draft Law No .....

(k) Inform the Cooperation Group of its activities and of the other forms of operational cooperation discussed pursuant to point (j) and request, where necessary, guidance in that regard;	
(l) Analyse the results of cybersecurity exercises, including those organised by ENISA;	
(m) At the request of a CSIRT, discuss its capabilities and preparedness;	
(n) Cooperate and exchange information with regional and Union-level security operations centres in order to improve common situational awareness of incidents and threats across the Union;	

(o) Where relevant, discuss the reports of the peer reviews referred to in Article 19(9);	
(p) Provide guidance in order to facilitate convergence of operational practices with regard to the application of the provisions of this Article on operational cooperation.	
4. By 17 January 2025, and every two years thereafter, the CSIRTs network shall assess the progress made in the area of operational cooperation and submit a report for the purposes of the evaluation referred to in Article 40. In particular, the report shall set out conclusions and make recommendations on the results of the peer reviews carried out pursuant to Article 19 in relation to national CSIRTs. That report shall be submitted to the Cooperation Group.	
5. The CSIRTs network shall	

adopt its rules of procedure. 6. The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis of those arrangements.	
Article 16 European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) 1. EU-CyCLONe is hereby established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information between Member States and Union institutions, bodies, offices and agencies. 2. EU-CyCLONe shall be composed of representatives of the cyber crisis management authorities of the Member States,	Article 39 Vulnerability reporting Where the vulnerability has a major impact on entities in more than one Member State of the European Union, 'CERT.PT' cooperates with its counterparts, either within the European Network of CSIRTs or within the EU-CyCLONe framework.

as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on the services and activities falling within the scope of this Directive, by the Commission. In other cases, the Commission participates in EU-CyCLONe activities as an observer. ENISA shall provide the EU-CyCLONe secretariat and support the secure exchange of information, as well as provide the necessary tools to support cooperation between Member States, ensuring the secure exchange of information. Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work. 3. The tasks of EU-CyCLONe shall be:	

Draft Law No .....

(a) Increase the level of preparedness for the management of large-scale cybersecurity incidents and crises;	
(b) Develop common situational awareness of large-scale cybersecurity incidents and crises;	
(c) Assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigating measures;	
(d) Coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;	

Draft Law No .....

(e) Discuss, at the request of the Member State concerned, the national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4). 4. EU-CyCLONe shall adopt its rules of procedure. 5. EU-CyCLONe shall report to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, paying particular attention to their impact on essential and important entities. 6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of the agreed procedural arrangements set out in Article 15(6). 7. By 17 July 2024, and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council an evaluation report on its work.	

Draft Law No .....

Article 17 International cooperation Where appropriate, the Union may conclude, in accordance with Article 218 TFEU, international agreements with third countries or international organisations, allowing and governing their participation in certain activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union law on data protection.	N/A
Article 18 Report on the state of cybersecurity in the Union 1. ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall transmit and submit that report to the European Parliament. That report shall, in particular, be	N/A

made available in a machine-readable format and shall include: (a) A cybersecurity risk assessment at Union level, taking into account the cyber threat landscape; (b) An assessment of the development of cybersecurity capacities in the public and private sectors across the Union; (c) An assessment of the general level of cybersecurity and cyber hygiene awareness among citizens and entities, including small and medium-sized enterprises; (d) An aggregated assessment of the results of the peer reviews referred to in Article 19;	

(e) An aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including at sectoral level, as well as the degree of alignment of Member States' national cybersecurity strategies. 2. The report shall include specific policy recommendations with a view to closing gaps and increasing the level of cybersecurity across the Union and a summary of the findings, for the period in question, of the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881. 3. ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs Network, shall develop the methodology, including relevant variables such as quantitative and qualitative indicators, of the aggregated assessment referred to in (1)(e).	

Draft Law No .....

Article 19 Peer reviews 1. No later than 17 January 2025, the Cooperation Group shall establish, with the assistance of the Commission and ENISA and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews, with a view to drawing lessons from shared experiences, enhancing mutual trust, achieving a high common level of cybersecurity and strengthening the cybersecurity capabilities and policies of the Member States necessary for the implementation of this Directive. Participation in peer reviews is voluntary. Peer reviews shall be carried out by cybersecurity experts. Cybersecurity experts shall be designated by at least two Member States, different from the evaluated Member State. Peer reviews shall address at least	N/A

one of the following: (a) The level of implementation of the cybersecurity risk-management measures and reporting obligations provided for in Articles 21 and 23; (b) The level of capabilities, including available financial, technical and human resources, and the effectiveness of the competent authorities in carrying out their tasks; (c) The operational capabilities of the CSIRTs; (d) The level of implementation of the mutual assistance referred to in Article 37;	

(e) The level of implementation of cybersecurity information sharing arrangements referred to in Article 29; (f) Specific issues of a cross-border or cross-sectoral nature. 2. The methodology referred to in (1) shall include objective, non-discriminatory, fair and transparent criteria on the basis of which Member States shall designate eligible cybersecurity experts to carry out the peer reviews. The Commission and ENISA shall participate in the peer reviews as observers. 3. Member States may identify specific issues referred to in (1)(f) for the purpose of peer review. 4. Before commencing a peer review as referred to in (1), Member States shall notify the participating Member States of the scope of that assessment, including the specific issues identified	

pursuant to (3). 5. Before the start of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall establish, with the assistance of the Commission and ENISA, the methodology for the self-assessment by the Member States. 6. Peer reviews should include virtual or physical site visits and off-site exchanges of information. Taking into account the principle of good cooperation, the Member States subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law relating to the protection of confidential or classified information and the safeguarding of essential State	

functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct on which to base the working methods of the designated cybersecurity experts. The information obtained during the peer review shall be used exclusively for that purpose. Cybersecurity experts participating in the peer review shall not disclose to third parties any sensitive or confidential information obtained in the course of the peer review. 7. Aspects that have been subject to a peer review in a Member State shall not be subject to a further peer review in that Member State within two years of the conclusion of the peer review, unless the Member State requests otherwise or decides otherwise following a proposal from the Cooperation Group.	

8. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed, prior to the start of the peer review, to the other Member States, the Cooperation Group, the Commission and ENISA. The Member State subject to a peer review may object to the designation of certain cybersecurity experts on duly substantiated grounds communicated to the designating Member State. 9. Cybersecurity experts participating in peer reviews shall report on the findings and conclusions of those peer reviews. The peer-reviewed Member States may comment on the draft reports concerning them and those comments shall be annexed to the reports. The reports shall include recommendations for improving the aspects covered by the peer review. The reports shall be	

submitted to the Cooperation Group and the CSIRTs network, where relevant. A Member State under peer review may decide to make public its report or a redacted version thereof.	
Article 20 Governance 1. Member States shall ensure that the governing bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in accordance with Article 21, supervise their implementation and may be held liable for infringements committed by the entities referred to in that Article. This paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions as	Article 25 Obligations of management, direction and administrative bodies 1 - The management, direction and administrative bodies of essential and important entities shall: a) Approve the cybersecurity risk-management measures adopted in accordance with Article 27; b) Oversee the implementation of cybersecurity risk management

well as the liability of public officials and elected or appointed officials. 2. Member States shall also ensure that members of the management body of essential and important entities are required to undergo training and encourage essential and important entities to regularly provide similar training to their employees in order to acquire sufficient knowledge and skills to identify and assess cybersecurity risk management practices and their impact on the services provided by the entity.	measures; c) Ensure compliance with the supervisory and enforcement measures referred to in Chapter VI of this Decree-Law; d) Ensure the regular conduct of cybersecurity training to promote an internal management culture on cybersecurity risk management practices. 2 - The holders of the management, direction and administrative bodies may be held liable by action or omission, intentionally or with serious fault, in accordance with the applicable legislation, for the infringements provided for in this Decree-Law.

Draft Law No .....

	3 - The responsibility and powers necessary for the fulfilment of the obligations referred to in this Article may not be delegated, except to one of the holders of the management, direction and administrative bodies.
Article 21 Cybersecurity risk management measures 1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the network and information systems they use in their operations or in the provision of their services and to prevent or minimise the impact of incidents on recipients of their	Article 26 Cybersecurity risk management system 1 - Essential and important entities shall be responsible for ensuring the security of network and information systems by taking appropriate technical, operational and organisational measures to manage the risks posed to the security of network and

Draft Law No .....

services and on other services The measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risk at stake, taking into account the latest technical progress and, where applicable, relevant European and international standards, as well as implementation costs When assessing the proportionality of such measures, due account shall be taken of the extent of the entity's exposure to risks, the size of the entity and the likelihood of occurrence of incidents and their severity, including their social and economic impact. 2. The measures referred to in (1) shall be based on an all-hazards approach aimed at protecting network and information systems and their physical environment from incidents, and shall cover at least the following aspects:	information systems that they use in their operations and to prevent or minimise the impact of incidents on recipients of their services and on other services. 2 - Cybersecurity measures adopted should be based on a systemic approach covering all risks for essential and important entities and aiming at protecting network and information systems as well as their physical environment from incidents. 3 - The measures should also: a) Ensure a level of security of network and information systems appropriate

(a) Risk analysis and information systems security policies; (b) Incident handling; (c) Business continuity, such as backup management and disaster recovery, and crisis management; (d) Supply chain security, including security aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) Security in the acquisition, development and maintenance of network and information systems, including vulnerability handling and disclosure; (f) Policies and procedures to assess the effectiveness of cybersecurity risk management measures;	to the risk at stake, taking into account the latest technical developments and, where applicable, relevant European and international standards, as well as their implementation costs and financial viability; and b) Be proportionate to the extent of the entity's exposure to risks, the size of the entity, and the probability of occurrence of incidents and their severity, including their social and economic impact, in accordance with the technical criteria to be defined by the CNCS.

Draft Law No .....

(g) Basic cyber hygiene practices and cybersecurity training; (h) Policies and procedures regarding the use of cryptography and, where applicable, encryption; (i) Human resources security, access control policies, and asset management; (j) Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications and secure emergency communications systems within the entity, where appropriate. 3. Member States shall ensure that when considering the appropriate measures referred to in (2)(d) of this Article, entities shall take into account the	4 - In order to guide the cybersecurity risk management policy of essential and important entities, the CNCS may issue technical harmonisation instructions and, where necessary, develop and update the risk matrix applicable to those entities. 5 - Considering the sector of activity and the size of the entity and the risk matrix defined, the CNCS, through [...], defines mini.mum and specific cybersecurity measures and levels of compliance, within the scope of the QNRCS, to be adopted by essential entities and important entities.

vulnerabilities specific to each direct supplier and service provider, as well as the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when assessing which of the measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out pursuant to Article 22(1). 4. Member States shall ensure that an entity concludes that it does not comply with the measures set out in (2) take all necessary, appropriate and proportionate corrective measures without undue delay. 5. By 17 October 2024, the Commission shall adopt	6 - The minimum cybersecurity measures shall be without prejudice to the adoption of other measures that are necessary and proportionate as a result of the analysis and management of residual cybersecurity risks, in accordance with the following Article. 7 - The relevant public entities shall adopt the appropriate technical, operational and organisational measures as determined by the CNCS, in accordance with the group to which they belong, pursuant to Article 33.

Draft Law No .....

implementing acts laying down the technical and methodological requirements for the measures referred to in (2) as regards DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms and trust service providers. The Commission may adopt implementing acts laying down the technical and methodological requirements, as well as the sector-specific requirements, where necessary, of the measures referred to in (2) in respect of essential and important entities other than those referred to in the first subparagraph of this paragraph.	Article 27 Cybersecurity measures 1 - The cybersecurity measures to be adopted by essential and important entities, taking into account the risk matrix in which they are inserted in accordance with Article 26, shall cover, *inter alia,* the following areas: j) incident handling; k) business continuity, such as backup management and disaster recovery, and crisis management; l) Supply chain security, including security aspects concerning the relationships between each entity

In preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, as far as possible, follow European and international standards as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4)(e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).	and its direct suppliers or service providers; m) Security in the acquisition, development and maintenance of network and information systems, including vulnerability handling and disclosure; n) Policies and procedures to assess the effectiveness of cybersecurity risk management measures; o) Basic cyber hygiene practices and cybersecurity training, including senior management and employees; p) Policies and

Draft Law No .....

	procedures relating to the use of cryptography and, where appropriate, encryption, without prejudice to the powers conferred on other entities in the field of cryptography at national level or before other international organisations of which Portugal is a member; q) Human resources security, access control policies, and asset management; r) Use of multi-factor authentication or continuous authentication, secure communications, and secure emergency

	communications systems within the entity. 2 - Essential and important entities shall also adopt, without undue delay, all necessary, appropriate and proportionate corrective cybersecurity measures that are indispensable for remedying failures or omissions in complying with the measures provided for in the preceding paragraph. 3 - Sectoral national cybersecurity authorities may issue regulatory provisions for sector-specific cybersecurity measures, without prejudice to the

	provisions of Article 20(3). Article 28 Supply chain Cybersecurity measures relating to supply chain security, including security aspects relating to the relationships between each entity and its direct suppliers or service providers, shall consider, *inter alia*: a) The vulnerabilities specific to each direct supplier and service provider; b) The overall quality of the products in the cybersecurity component; c) The cybersecurity practices of their suppliers and service providers, including

	their secure development procedures; d) The coordinated security risk assessments of supply chains of critical ICT products, ICT systems or ICT services that are carried out pursuant to Article 22 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December; e) Decisions on the application of restrictions on the use, cessation of use or exclusion of information and communication technology equipment, components or services pursuant to Article 18(3).

Draft Law No .....

Article 22 Union coordinated assessments of security risks of critical supply chains 1. In cooperation with the Commission and ENISA, the Cooperation Group may carry out coordinated security risk assessments of supply chains of critical ICT products, ICT systems or ICT services, taking into account technical and, where relevant, non-technical risk factors. 2. After consulting the Cooperation Group and ENISA and, where necessary, relevant stakeholders, the Commission shall identify the specific critical ICT products, ICT systems or ICT services that may be subject to the coordinated security risk assessment referred to in (1).	N/A
Article 23 Notification obligations	Article 40 Mandatory notification

Draft Law No .....

1. Member States shall ensure that essential and important entities notify their CSIRT or, where applicable, their competent authority, without undue delay and in accordance with (4) of any incident having a significant impact on the provision of its services as referred to in (3) (significant incident). Where appropriate, the entities concerned shall notify the recipients of their services without undue delay of significant incidents that may negatively affect the provision of those services. Each Member State shall ensure that those entities report, *inter alia*, any information enabling the CSIRT or, where applicable, the competent authority to determine the possible cross-border impact of the incident. Mere notification does not subject the notifying entity to increased responsibilities. Where the entities concerned notify the competent authority of a significant incident pursuant to the	1 - Essential, important, and relevant public entities shall notify any significant incident to the competent cybersecurity authority. 2 - Compliance with the mere notification does not give rise to increased liability on the part of the notifying entity. 3 - In determining whether an incident has a significant impact pursuant to paragraph 1, the entities concerned shall take into account, *inter alia*, the following parameters: a) Number of users affected by the service disruption;

first subparagraph, the Member State shall ensure that that competent authority transmits the notification to the CSIRT upon receipt. In the event of a significant cross-border or cross-sectoral incident, Member States shall ensure that their Single Points of Contact receive the relevant information notified in accordance with (4) in a timely manner. 2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to recipients of their services potentially affected by a significant cyber threat, the measures or remedies that they can take to address that threat. Where appropriate, entities shall also inform those recipients of the significant cyber threat itself. 3. An incident shall be deemed significant if:	b) The duration of the incident; c) The level of severity of the disruption to the operation of the service; d) The extent of the impact on economic and social activities. 4 - Entities should also take into consideration the parameters and thresholds defined by technical instruction of the CNCS and by the Commission implementing acts, provided for in Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December.

Draft Law No .....

(a) Has caused or is likely to cause serious operational disruption of services or financial loss to the entity concerned; (b) Has affected or is likely to affect other natural or legal persons by causing considerable material or non-material damage. 4. Member States shall ensure that, for the purposes of the notification provided for in (1), the entities concerned shall submit to the CSIRT or, where applicable, to the competent authority: (a) Without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by an unlawful or malicious act or whether it may have a cross-border impact;	5 - Compliance with the provisions of this Decree-Law shall not exempt compliance with specific incident notification obligations as defined by the competent authorities, namely the Public Prosecutor's Office, the Judicial Police, the National Data Protection Commission (CNPD), the State Secret Supervisory Authority and the GNS, in accordance with the applicable legal and regulatory provisions. 6 - Notifications shall be submitted on the electronic platform referred to in Article 8(7). 7 - Relevant essential, important and

(b) Without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and provide an initial assessment of the significant incident, including its severity and impact, as well as, where available, indicators of exposure to risks; (c) At the request of a CSIRT or, where applicable, the competent authority, an interim report containing important updates on the situation;	public entities shall be ensured the possibility to notify an incident simultaneously to the competent cybersecurity authority, to the special cybersecurity authorities, as well as to the entities referred to in paragraph 5 of this Article, through the platform provided for in Article 8(7), in accordance with a protocol to be established between those authorities. Article 41 Types of notifications 1 - For each incident subject to mandatory notification, relevant essential, important, and public entities shall

Draft Law No .....

(d) No later than one month after the submission of the incident notification referred to in point (b), a final report containing the following: (i) A detailed description of the incident, including its severity and impact; (ii) The type of threat or likely primary cause likely to have triggered the incident; (iii) Implemented and ongoing mitigation measures; (iv) Where applicable, the cross-border impact of the incident;	submit: a) An initial notification in accordance with Article 42; b) A notification of the end of the significant impact pursuant to Article 43; c) A final report in accordance with Article 44. 2 - In cases where the incident is resolved within two hours of its detection, the entities referred to are only required to send the notification of the end of significant impact. 3 - Without prejudice to the provisions of the preceding paragraph, relevant essential, important and public

(eIn the event of an ongoing) incident at the time of submission of the final report referred to in point (d), Member States shall ensure that the entities concerned submit an interim report at that time and a final report within one month of resolving the incident. By way of derogation from point (b) of the first subparagraph, a trust service provider shall notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident, of any significant incident affecting the provision of its trust services. 5. without undue delay and, where possible, within 24 hours of receipt of the early warning referred to in (4)(a), the CSIRT or the competent authority shall provide a response to the reporting entity providing, *inter alia*, its initial comments on the significant	entities may still be notified to submit an interim report, pursuant to Article 44. 4 - The incident notification format and procedure and the taxonomy of incidents, including the categories of causes of incidents and their effects, shall be defined by technical instruction of the CNCS, without prejudice to the implementing acts adopted by the Commission provided for in Article 23(11) of Directive (EU) 2022/2555. Article 42 Initial notification 1 - The initial notification shall be

incident and, at the request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the original recipient of the notification referred to in (1), the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if requested by the entity concerned. In cases where the criminal nature of the significant incident is suspected, the CSIRT or the competent authority shall also provide guidance on the reporting of the significant incident to law enforcement authorities. 6. Where applicable, and in particular whether the significant incident referred to in (1) concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and	sent to the relevant cybersecurity authority as soon as the relevant essential, important or public entity concludes that a significant incident exists or is likely to occur, without undue delay and no later than 24 hours after that verification, unless this is incompatible with mitigating or resolving the incident. 2 - The initial notification shall include at least the following information: a) The name, telephone number and email address of a representative of the entity, where different from the permanent point of

ENISA of the significant incident. Such information shall include the type of information received in accordance with (4). In doing so, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, safeguard the security and commercial interests of the entity and the confidentiality of the information provided. 7. Where public awareness is necessary to prevent a significant incident or to respond to an ongoing significant incident, or where disclosure of the significant incident is in the public interest, the CSIRT of a Member State or, where applicable, its competent authority and, where applicable, the CSIRTs or the competent authorities of other affected Member States may, after consulting the entity concerned, inform the public of the significant incident or require the entity to do so.	contact referred to in Article 32, for the purpose of any contact by the competent cybersecurity authority; b) The date and time of the start or, if this cannot be determined, of the detection of the incident; c) A brief description of the incident, including an indication of the category of cause and effects produced, according to the taxonomy defined by the CNCS, where possible, the respective detail; d) Possible estimation

Draft Law No .....

8. At the request of the CSIRT or the competent authority, the single point of contact shall transmit the notifications received pursuant to (1) to the Single Points of Contact of the other affected Member States. 9. The Single Point of Contact shall submit a summary report to ENISA every three months, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified pursuant to (1) of this Article and of Article 30 In order to contribute to the comparability of the information submitted, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs Network of its findings on the notifications received every six months.	of the impact, considering: i) Number of users affected by the service disruption; ii) Duration of the incident; iii) Geographical distribution, as regards the area affected by the incident, including an indication of the cross-border impact; iv) Other information that the essential and important entity considers

Draft Law No .....

10. CSIRTs or, where applicable, competent authorities shall provide competent authorities pursuant to Directive (EU) 2022/2557 with information on significant incidents, incidents, cyber threats and near misses notified pursuant to p(1) of this Article and of Article 30 entities identified as critical entities pursuant to Directive (EU) 2022/2557. 11. The Commission may adopt implementing acts specifying the type of information, the format and the procedure for notifications submitted pursuant to (1) of this Article and of Article 30 and communications made pursuant to (2) of this article. By 17 October 2024, the Commission shall, as regards DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service	relevant. 3 - Where necessary, the relevant essential, important or public entity shall send to the competent cybersecurity authority an update of the initial notification no later than 72 hours after the verification of the significant incident, reviewing the information referred to in the previous paragraph and providing an initial assessment of the significant incident, including its severity and impact, as well as, where available, indicators of exposure to risks. Article 43 Notification of the end of

providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, adopt implementing acts specifying the cases in which an incident is to be considered significant as referred to in (3). The Commission may adopt implementing acts in respect of other essential and important entities. The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs in accordance with Article 14(4)(e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).	significant impact 1 - The notification of the end of the significant impact of the incident shall be submitted to the competent cybersecurity authority, without undue delay and within 24 hours of the end of the impact. 2 - The notification of the end of significant impact shall include at least the following information: a) Updating the information transmitted in the initial notification, if any; b) A brief description of the measures taken to resolve the incident;

Draft Law No .....

	c) Description of the impact situation existing at the time of the loss of significant impact, including: i) Number of users affected by the service disruption; ii) Duration of the incident; iii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact; iv) Estimated time for full recovery of services.

Draft Law No .....

	Article 44 Final and interim reports 1 - The final report shall be submitted to the competent cybersecurity authority within 30 working days from the date of notification of the end of the significant impact of the incident. 2 - The final report shall include the following information: a) The date and time when the incident assumed the significant impact; b) The date and

	time when the incident lost its significant impact; c) Impact of the incident, considering: i) Number of users affected by the service disruption; ii) Duration of the incident; iii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact; iv) Description of the incident, indicating the

Draft Law No .....

	category of cause and effects produced, according to the taxonomy defined by the CNCS, and the respective details; d) An indication of the measures taken to mitigate the incident; e) Description of the residual impact situation existing at the time of the final notification, in particular: i) Number of users affected by the service

Draft Law No .....

	disruption; ii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border impact; iii) Estimated time for full recovery of services still affected; iv) Indication, where applicable, of the submission of notification of the incident in question to the competent

Draft Law No .....

	authorities, namely the Public Prosecutor's Office or the CNPD and other sectoral authorities, in accordance with the applicable laws and regulations; v) Other information that the essential and important entity considers relevant. 3 - In the event that, after the deadline for submission of the final report, the incident is still

	ongoing, the relevant essential, important or public entity concerned shall submit an interim report to the competent cybersecurity authority, at the request of those entities and on a weekly basis until the time the final report is submitted. 4 - The interim report shall include the following information: a) Updating the information transmitted in the initial notification, if any; b) A brief description of

	the measures taken to resolve the incident; c) Description of the impact situation existing at the time of the loss of significant impact, including: i) Number of users affected by the service disruption; ii) Duration of the incident; iii) Geographical distribution, as regards the area affected by the incident, including indication of cross-border

Draft Law No .....

	impact; iv) Estimated time for full recovery of services. Article 45. Voluntary notifications of relevant information 1 - Without prejudice to the incident notification obligation provided for in this Decree-Law, any natural or legal person may notify, on a voluntary basis, the occurrence of incidents, cyber threats, near misses or vulnerabilities. 2 - Voluntary notifications do not create additional obligations for the

Draft Law No .....

	notifying entity. 3 - Articles 42 to 44 shall apply *mutatis mutandis* to voluntary notifications, without prejudice to the priority to be given to the processing of mandatory notifications. Article 46 Enquiries The competent cybersecurity authority may request relevant information from the relevant essential, important or public entities or determine the necessary actions, in accordance with the law, when it becomes aware, by any means, of a potential incident and Articles 42 to 44 shall apply *mutatis mutandis*.

Draft Law No .....

	Article 47 Information protection 1 - The sending of information by the CNCS or, where applicable, by the national sectoral cybersecurity authorities, under this Decree-Law, to competent national authorities or entities of the European Union or of another Member State is limited to what is necessary and proportionate, in accordance with the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No 58/2019 of 8

Draft Law No .....

	August, and Law No 59/2019 of 8 August. 2 - The competent cybersecurity authority shall ensure the adequate protection of information and data, of whatever nature, transmitted by essential, important and public entities relevant to confidentiality and trade secrets. 3 - Paragraph 2 shall apply *mutatis mutandis* to information provided by natural and legal persons making a notification under the preceding Article. Article 48 Communication to recipients of services 1 - Relevant

Draft Law No .....

	essential, important and public entities shall report to the recipients of their services, without undue delay, any incidents with a significant impact that are likely to negatively affect them. 2 - Relevant essential, important and public entities shall report to the recipients of their services potentially affected by a significant cyber threat, without undue delay, the measures or solutions that they can adopt to respond to the threat and, where appropriate, communicate to them the cyber threat concerned. 3 - The

Draft Law No .....

	communication referred to in the preceding paragraph shall not relieve the entities concerned of their duty, at their own expense, to take appropriate and immediate measures to prevent or remedy any threats and to restore the normal level of security of the service they provide. 4 - The information referred to in the preceding paragraphs shall be provided free of charge and in easily understandable language. Section III Incident reporting, public information and response

Draft Law No .....

	Article 49 Communication between authorities 1 - Sectoral and special national cybersecurity authorities shall report to the CNCS all incidents of which they are notified in accordance with Article 40, and shall inform the CNCS of their progress. 2 - For the purposes of Article 21, the CNCS shall report to the Secretary-General of the Internal Security System, without undue delay, incidents of which they are notified in accordance with Article 40 that are likely to qualify as large-scale. 3 - The CNCS shall,

Draft Law No .....

	where it deems it necessary, inform the sectoral and special national cybersecurity authorities of voluntary notifications pursuant to Article 45. 4 - This Article shall apply *mutatis mutandis* to notifications made pursuant to Article 42. 5 - The communications referred to in the preceding paragraphs shall be made immediately by electronic means. Article 50 Communication to entities within the European Union or its Member States 1 - Where justified, in particular where a

	significant incident involves at least one other Member State of the European Union, the CNCS shall inform the other affected Member States designated under Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December and ENISA of the occurrence of the significant incident, ensuring that existing cooperation channels on police cooperation and intelligence services are respected. 2 - The communication referred to in the preceding paragraph shall include the information received through the notifications made

	pursuant to Articles 42 et seq. 3 - The CNCS, as the single point of contact, shall submit a quarterly summary report to ENISA, including anonymised and aggregated data on significant incidents, incidents, cyber threats, and near misses notified pursuant to Articles 40 and 45. Article 51 Information to the public 1 - The competent cybersecurity authority shall inform the public of the occurrence of a significant incident, after consultation with the entity concerned,

Draft Law No .....

	where: c) There is a need for public clarification to prevent the incident or to respond to an ongoing incident; d) Disclosure of the significant incident is in the public interest. 2 - The competent cybersecurity authority shall also require the entity concerned to disclose the significant incident to the public where the situations referred to in the previous paragraph are concerned. 3 - The competent cybersecurity authority shall inform the public of a significant incident at the request of a

	competent authority of another Member State of the European Union. 4 - The communication to the public provided for in this Article shall be without prejudice to cooperation in ongoing criminal investigations or those covered by the rules on judicial and State secrecy. Article 52 Reply to notifications 6 - The competent cybersecurity authority shall reply to the notifying entity without undue delay and, where possible, within 24 hours of receiving the initial notification provided for in Article

	42. 7 - The competent cybersecurity authority shall provide in its response, *inter alia*, its initial comments on the significant incident and, at the request of the entity, guidance or operational advice on the implementation of possible mitigating measures. 8 - In situations of serious and proven risk of the impact of the incident notified pursuant to Article 40, the competent cybersecurity authority may impose, as an immediate enforcement measure, the interruption of the provision of service to the relevant essential,

	important or public entity concerned, or the cessation of conduct that infringes this Decree-Law, if it does not do so on a voluntary basis. 9 - In cases of well-founded suspicion of the criminal nature of the significant incident, the competent cybersecurity authority shall also provide guidance on the notification of the significant incident to law enforcement authorities. 10 - The provisions of the preceding paragraphs shall apply *mutatis mutandis* to incidents, near misses or cyber threats that have been notified on a

Draft Law No .....

	voluntary basis under Article 45.
Article 24 Use of European cybersecurity certification regimes 1. In order to demonstrate compliance with certain requirements set out in Article 21, Member States may require essential and important entities to use certain ICT products, ICT services and ICT processes, developed by the essential or important entity or provided by a third party, that are certified under European cybersecurity certification regimes adopted pursuant to Article 49 of Regulation (EU) 2019/881. In addition, Member States should encourage essential and important entities to use qualified trust services. 2. The Commission shall be empowered to adopt delegated acts	Article 34 Cybersecurity certification 3 - The CNCS may require essential, important and relevant public entities to obtain certification in cybersecurity, national or European, attesting compliance with the cybersecurity measures of this Decree-Law, namely in accordance with certification regimes drawn up from the Portuguese Normative Document - Technical Specification (DNP TS) 4577-1, Digital Maturity - Digital Seal and the National Reference Framework for

Draft Law No .....

in accordance with Article 38 to supplement this Directive by specifying the categories of essential and important entities required to use certified ICT products, ICT services and ICT processes or to obtain a certificate under a European cybersecurity regime adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity are identified and shall include an implementation period. Before adopting such delegated acts, the Commission shall carry out an impact assessment and carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881. 3. Where there is no suitable European cybersecurity certification regime for the purposes of (2) of this Article, the Commission, after consulting the	Cybersecurity. 4 - The CNCS may also require relevant essential, important and public entities, pursuant to Article 24(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, to use ICT products, services and processes, all developed by the entity or provided by third parties, certified under national and European cybersecurity certification regimes adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April.

Cooperation Group and the European Cybersecurity Certification Group, may request ENISA to prepare a candidate regime in accordance with Article 48(2) of Regulation (EU) 2019/881.	
Article 25 Standardisation 1. In order to promote the convergent application of Article 21(1) and (2) Member States shall encourage, without imposing or discriminating in favour of the use of a particular type of technology, the use of European and international standards and technical specifications applicable to the security of network and information systems. 2. ENISA shall, in cooperation with the Member States and, where appropriate, after consulting relevant stakeholders, issue recommendations and guidelines on the technical areas to be	Article 34 Cybersecurity certification 1 - The CNCS may require essential, important and relevant public entities to obtain certification in cybersecurity, national or European, attesting compliance with the cybersecurity measures of this Decree-Law, namely in accordance with certification regimes drawn up from the Portuguese Normative Document - Technical Specification (DNP TS) 4577-1,

considered under (1), as well as on existing rules, including national rules, which would allow to cover these areas.	Digital Maturity - Digital Seal and the National Reference Framework for Cybersecurity. 2 - The CNCS may also require relevant essential, important and public entities, pursuant to Article 24(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December, to use ICT products, services and processes, all developed by the entity or provided by third parties, certified under national and European cybersecurity certification regimes adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament

Draft Law No .....

	and of the Council of 17 April.
Article 26 Competence and territoriality 1. Entities falling within the scope of this Directive shall be deemed to fall under the jurisdiction of the Member State in which they are established, except for: (a) Providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;	Article 4 Territorial delimitation of the subjective scope 4 - This Decree-Law shall apply to the entities referred to in (1) and (2) of the preceding Article which: *d)* Have an establishment in the national territory; *e)* In the case of undertakings providing public electronic communications networks or publicly available electronic communications services, they shall provide such

(b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union in accordance with (2).	services within the national territory;
Article 27 Registration of entities 1. ENISA shall establish and maintain a register of DNS service providers, TLD name registries, entities providing domain name	Article 35 Enrolment Duty 5 - For the purposes of registration, relevant essential, important and public entities have the duty to enter in the

registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, based on the information received from the single points of contact in accordance with (4). Upon request, ENISA shall allow competent authorities access to that register, while ensuring the protection of the confidentiality of information, where applicable. 2. By 17 January 2025 at the latest, Member States shall require the entities referred to in (1) submit the following information to the competent authorities: (a) Entity name;	electronic platform referred to in Article 8(7) the elements that allow their complete identification, namely f) The name of the entity concerned; g) Tax number, h) Up-to-date address and contact details, including e-mail addresses, IP address ranges and telephone numbers; i) Where applicable, the relevant sector and subsector referred to in Annexes I or II to this Decree-Law, which form an integral part

(b) The sector, subsector and type of entity referred to in Annex I or II, if applicable; (c) Address of the main establishment of the entity and its other legal establishments in the Union or, if not established in the Union, of its representative designated in accordance with Article 26(3); (d) up-to-date contacts, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3); (e) Member States where the entity provides services; and (f) Ranges of IP addresses of the entity. 3. Member States shall ensure	thereof; and j) Where applicable, a list of the Member States of the European Union in which they provide services falling within the scope of this Decree-Law. 6 - In addition to the data referred to in the previous paragraph, the registration of top-level domain names, as well as entities that are DNS service providers, domain name registration service providers, cloud computing service providers, data centre service providers, content delivery network providers,

that the entities referred to in (1) notify the competent authority of changes in the information they have provided pursuant to (2), without delay and in any event within three months of the date of the amendment. 4. upon receipt of the information referred to in (2) and (3), other than that referred to in (2)(f), the single point of contact of the Member State concerned shall transmit that information to ENISA without undue delay. 5. Where applicable, the information referred to in p(2) and (3) of this Article shall be transmitted through the national mechanism referred to in Article 3(4).	managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, have the duty to register the following elements on the electronic platform referred to in Article 8(7): e) The address of its principal place of business and other legal establishments in the European Union or, where it is not established in the Union, of its designated representative;

Draft Law No .....

	f) Up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its designated representative; g) The Member States in which it provides services; and h) The ranges of IP addresses. 7 - Relevant essential, important, public entities and domain name registries service providers shall notify any change to the data referred to in the preceding paragraphs within 30 working days

	of the change. 8 - In the case of registering TLD names, as well as entities that are DNS service providers, domain name registration service providers, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking service platforms, the change to the data referred to in (1) and (2) shall be notified within three months of

Draft Law No .....

	the change.
Article 28 Domain name registration database 1. With a view to contributing to the security, stability and resilience of the DNS, Member States should require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards personal data. 2. For the purposes of (1), Member States shall require that the domain name registration database contains the information necessary to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLD. That information shall include:	Article 36 Domain name registration database 6 - The TLD name registry and the entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data in purpose-built databases. 7 - The collection and maintenance of the data referred to in the preceding paragraph constitutes a legal obligation under and for the purposes of Article 6(1)(c) of the GDPR. 8 - The database

Draft Law No .....

(a) The domain name; (b) The date of registration, (c) The name, contact email address and telephone number of the applicant for registration; (d) The contact email address and telephone number of the point of contact administering the domain name, if different from those of the registrant. 3. Member States shall also require TLD name registries and entities providing domain name registration services to have in place policies and procedures, including verification procedures, to ensure that the databases referred to in (1) are maintained contains accurate and complete information. Member States shall require those policies and procedures to be made public.	referred to in (1) shall contain the following information: e) The domain name; f) The date of registration, g) The name, contact email address and telephone number of the registration holder; h) The contact address and the contact telephone number administering the domain name, if different from the registration holder. 9 - The TLD name

4. Member States shall require TLD name registries and entities providing domain name registration services to those registries to make public, without undue delay after the registration of a domain name, domain name registration data other than personal data,	registry and the entities providing domain services shall adopt policies and procedures, including verification, to ensure that their databases, in accordance with (1), contain accurate and complete information.
5. Member States shall require TLD name registries and entities providing domain name registration services to grant access to specific domain name registration data to legitimate access seekers who make a lawful and duly reasoned request, in accordance with Union data protection law, Member States shall require TLD name registries and entities providing domain name registration services to respond without undue delay and in any event within 72 hours of receiving access requests. Member States shall require that policies and procedures for the	10 - The data relating to the registration of domain names and the policies and procedures referred to in the preceding paragraphs must be accessible to the public, when they are not personal data and are not protected under the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, in its current wording, Law No

dissemination of such data are made public. 6. the fulfilment of the obligations laid down in (1) to (5) shall not result in a duplication of the collection of domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.	58/2019 of 8 August and Law No 59/2019 of 8 August. Article 37 Access to domain name registration 3 - The registration of top-level domain names and entities providing domain name registration services guarantee access to specific data relating to the registration of domain names to those who submit a lawful and duly substantiated request for access, in accordance with the applicable legislation on the protection of personal data, namely the GDPR, Law No 26/2016 of 22 August, as amended, Law No

Draft Law No .....

	58/2019 of 8 August, and Law No 59/2019 of 8 August. 4 - Requests for access referred to in the preceding paragraph shall be granted within 72 hours of receipt thereof.
Article 29. Cybersecurity information sharing agreements 1. Member States shall ensure that entities falling within the scope of this Directive, as well as, where relevant, other entities not falling within the scope of this Directive, may exchange, on a voluntary basis, relevant cybersecurity information, including information related to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of risk exposure, hostile tactics, threat-	Article 24 Cooperation with the private sector 1 - Entities that are part of the institutional framework for cyberspace security, in accordance with Article 15, shall establish cooperative relations with the entities covered by this Decree-Law and, where relevant, with other private sector stakeholders, with a

specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools for the detection of cyber-attacks, provided that such information sharing: (a) Aims to prevent, detect, respond to and recover from incidents or mitigate their impact;	view to achieving the objectives of the cybersecurity legal regime. 2 - Cooperation relations shall cover at least the following aspects relating to the sharing of information, the adoption of best practices, the development or improvement of common or standardised classification systems and taxonomies with regard to: a) Cybersecurity risk management measures; b) Indicators of exposure to risks or cyber threats; c) Incident handling procedures;

(b) Enhance the level of cybersecurity, in particular by raising awareness of cyber threats, limiting or impeding their dissemination capacity, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies or response and recovery phases, or promoting collaborative investigation of cyber threats between public and private entities. 2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities and, where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information sharing arrangements that protect the potentially sensitive nature of	d) Crisis management; and e) Coordinated vulnerability disclosure in accordance with Article 38. 3 - In order to promote the exchange of knowledge, the sharing of best practices and the mobilisation of expertise from private sector entities in support of the relevant cybersecurity authority, public-private partnerships for cybersecurity may be adopted, defining the scope and the parties involved, the governance model, the available funding

the information shared. 3. Member States shall facilitate the conclusion of cybersecurity information-sharing arrangements referred to in (2) of this article. Such arrangements may specify the operational elements, including the use of dedicated ICT platforms and automation tools, the content and conditions of the information-sharing arrangements. When defining the details of the involvement of public authorities in such agreements, Member States may impose conditions on the information made available by competent authorities or CSIRTs. Member States shall offer assistance in the implementation of such agreements in accordance with their policies referred to in Article 7(2)(h). 4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in	options and the interaction between the participating parties. 4 - Cybersecurity information sharing agreements may be concluded between the entities referred to in paragraph 1 as well as, where relevant, with their suppliers or service providers, for the following purposes: a) Preventing, detecting, responding to, and recovering from incidents or mitigating their impact; b) Enhancing the level of cybersecurity, in particular by raising awareness of cyber threats, limiting or impeding their

the cybersecurity information-sharing arrangements referred to in (2) at the time of its conclusion or, where applicable, its withdrawal from such agreements, as soon as it takes effect. 5. ENISA shall assist in the conclusion of the cybersecurity information-sharing arrangements referred to in (2), exchanging best practices and providing guidance.	dissemination capacity, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies or response and recovery phases, or promoting collaborative investigation of cyber threats between public and private entities. 5 - The parties to the information-sharing agreements shall, where necessary, take measures to protect the sensitive nature of the information shared and

	limit its distribution, in accordance with the so-called TLP (Traffic Light Protocol). 6 - Essential and important entities are required to notify the competent cybersecurity authority of their participation in the agreements referred to in paragraph 4 at the time of their conclusion or, where applicable, of their withdrawal from such agreements, as soon as it becomes effective. 7 - The agreements referred to in paragraph 4, when concluded by essential and important entities covered by Regulation (EU) 2022/2554 of the

Draft Law No .....

	European Parliament and of the Council of 14 December on digital operational resilience for the financial sector, shall be communicated to the respective national special cybersecurity authorities. 8 - The CNCS ensures and manages an online platform for information sharing.
Article 30 Voluntary notification of relevant information 1. Member States shall ensure that, in addition to the notification obligation laid down in Article 23, notifications can be submitted to the CSIRTs or, where applicable, to the competent authorities, on a voluntary basis, by:	Article 45. Voluntary notifications of relevant information 1 - Without prejudice to the incident notification obligation provided for in this Decree-Law, any natural or legal person may notify, on a voluntary basis, the

Draft Law No .....

(a) Essential and important entities in case of incidents, cyber threats and near misses; (b) Entities other than those referred to in point (a), whether or not they fall within the scope of this Directive, in the event of significant incidents, cyber threats and near misses. 2. Member States shall process the notifications referred to in (1) of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with information on notifications received pursuant to this Article, while ensuring the confidentiality and adequate protection of the information	occurrence of incidents, cyber threats, near misses or vulnerabilities. 2 - Voluntary notifications do not create additional obligations for the notifying entity. 3 - Articles 42 to 44 shall apply *mutatis mutandis* to voluntary notifications, without prejudice to the priority to be given to the processing of mandatory notifications.

provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary notification shall not result in the imposition of any additional obligations on the reporting entity to which it would not have been subject if it had not submitted the notification.	
Article 31 General aspects of supervision and enforcement 1. Member States shall ensure that their competent authorities effectively monitor compliance with this Directive and take the necessary measures to ensure such compliance. 2. Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation should be based on a risk-based approach. For this purpose, in the exercise of its	Article 53 Principles 6 - The competent cybersecurity authority, as the supervisory and enforcement authority, shall monitor and supervise compliance with this Decree-Law and take the necessary measures to ensure such compliance. 7 - Supervisory and enforcement activities shall be guided, *inter*

Draft Law No .....

supervisory functions under Articles 32 and 33, competent authorities may establish supervisory methodologies to prioritise those functions according to a risk-based approach. 3. When dealing with incidents that have led to personal data breaches, competent authorities should work in close cooperation with supervisory authorities under Regulation (EU) 2016/679, without prejudice to the competences and tasks of supervisory authorities under that Regulation. 4. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, when supervising the compliance of public administration entities with this Directive and imposing enforcement measures in respect of infringements of this Directive, competent authorities have the appropriate powers to carry out those tasks with	*alia*, by the principles of public interest, legality, efficiency, effectiveness and proportionality and shall minimise, where possible, their impact on the public, social and business activities of the supervised entities. 8 - Supervisory activity shall be based on risk assessment methodologies and, on the basis of that assessment and the principles referred to in the preceding paragraph, may determine the priority allocation of resources and the measures to be taken in accordance with the risk matrix applicable to the entity concerned, in particular as regards the conduct,

operational independence from the public administration entities supervised. Member States may decide to impose appropriate, proportionate and effective supervisory and enforcement measures in respect of such entities in accordance with national legislative and institutional frameworks.	frequency or type of on-site inspections, specific security audits or security checks and the type of information to be requested. 9 - Supervisory and enforcement activities shall be carried out with operational autonomy, including those targeting the relevant public entities. 10 - Supervisory and enforcement activities shall respect the legal and constitutional guarantees of individuals.
Article 32 Supervisory and enforcement measures in relation to essential entities	Article 53 Principles 1 - The competent cybersecurity authority,

Draft Law No .....

1. Member States shall ensure that supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case. 2. Member States shall ensure that, when carrying out their supervisory tasks in relation to essential entities, competent authorities have the power to subject those entities to at least: (a) On-site inspections and remote supervision, including random checks by qualified professionals; (b) Regular and targeted security audits carried out by an independent body or a competent authority;	as the supervisory and enforcement authority, shall monitor and supervise compliance with this Decree-Law and take the necessary measures to ensure such compliance. 2 - Supervisory and enforcement activities shall be guided, *inter alia*, by the principles of public interest, legality, efficiency, effectiveness and proportionality and shall minimise, where possible, their impact on the public, social and business activities of the supervised entities. 3 - Supervisory activity shall be based on risk assessment methodologies and, on the basis of that

Draft Law No .....

(c) Ad-hoc audits, including in cases justified by a significant incident or infringement of this Directive by the essential entity;	assessment and the principles referred to in the preceding paragraph, may determine the priority allocation of resources and the measures to be taken in accordance with the risk matrix applicable to the entity concerned, in particular as regards the conduct, frequency or type of on-site inspections, specific security audits or security checks and the type of information to be requested.
(d) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate in cooperation with the entity concerned;	4 - Supervisory and enforcement activities shall be carried out with operational autonomy, including those targeting the relevant public entities.
(e) Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;	5 - Supervisory and

Draft Law No .....

(f) Requests for access to data, documents and information necessary for the performance of supervisory tasks; (g) Requests for evidence of the implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and their underlying evidence. The specific security audits referred to in point (b) of the first subparagraph shall be based on risk assessments carried out by the competent authority or the audited entity, or other available risk-related information. The results of the specific security audits shall be made available to the competent authority. The costs of specific security audits carried out by an independent body shall be paid by the audited entity, except in duly justified cases where the competent authority decides	enforcement activities shall respect the legal and constitutional guarantees of individuals. Article 54 Supervisory measures concerning essential entities 1 - The competent cybersecurity authority shall have the power to subject essential entities to the following measures: a) On-site inspections and remote supervision, including random checks by qualified professionals; b) Regular or targeted security audits carried out by the competent authority

otherwise. 3. When exercising the powers provided for in (2)(e), (f) or (g), the competent authorities shall indicate the purpose of the request and specify the information requested. 4. Member States shall ensure that, when exercising their enforcement powers in relation to essential entities, their competent authorities have the power to at least: (a) Issue warnings about infringements of this Directive by the entities concerned;	itself or, where appropriate, by an entity appropriately qualified for that purpose and offering guarantees of independence; c) Ad-hoc audits, in particular on the basis of the verification of a significant incident, non-compliance by the competent cybersecurity authority or infringement of this Decree-Law by the entity concerned; d) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate in

Draft Law No .....

(b) Adopt binding instructions, including in relation to the measures necessary to prevent or remedy an incident, as well as the time limits for implementing those measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or infringements of this Directive; (c) Order the entities concerned to cease conduct that infringes this Directive and to refrain from repeating such conduct; (d) Order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or comply with the notification obligations set out in Article 23 in a specified manner and within a specified period;	cooperation with the entity concerned; e) Requests for information necessary to assess compliance with the cybersecurity measures referred to in Articles 27 et seq. adopted by the entity concerned; f) Requests for access to data, documents and information necessary for the performance of their supervisory tasks; g) Requests to provide evidence demonstrating the implementation of cybersecurity policies and procedures. 2 - The targeted audits referred to in (1)

Draft Law No .....

(e) Order the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities that are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures that may be taken by those persons in response to that threat;	(b) shall be based on the risk analysis carried out by the competent cybersecurity authority, the risk analysis carried out by the audited entity or other available risk-related information, including those contained in the technical harmonisation instructions and risk matrices prepared by the CNCS pursuant to Article 26(3), as well as the orders, instructions and guidelines of the competent cybersecurity authority.
(f) Order the entities concerned to implement, within a reasonable period of time, the recommendations made as a result of a security audit;	
(g) Designate a supervisor with well-defined tasks for a certain period of time to supervise the compliance of the entities concerned with Articles 21 and 23;	3 - The costs of targeted audits referred to in (1)(b) shall be borne by the audited entity, unless a reasoned decision to the contrary is taken by the competent

(h) Order the entities concerned to make public the aspects of infringements of this Directive in a specified manner;	cybersecurity authority. 4 - Requests for information and evidence referred to in (1)(e) to (g) shall state the purpose of the request, specify the information requested and set an appropriate and reasonable time limit for the essential entity to respond.
(i) Impose or request the imposition by the competent bodies or courts, in accordance with national law, of an administrative fine pursuant to Article 34, in addition to any of the measures referred to in points (a) to (h) of this paragraph.	
5. Where the implementing measures adopted pursuant to (4) (a) to (d) and (f) prove ineffective, Member States shall ensure that their competent authorities have the power to set a time limit within which the essential entity is requested to take the necessary measures to remedy the deficiencies or comply with the requirements of those authorities. Where the requested measure is not taken within the time limit,	Article 56 Implementing measures 1 - The competent cybersecurity authority may, in relation to essential, important and relevant public entities, adopt measures that include the following: a) Warnings of breaches of the obligations

Draft Law No .....

Member States shall ensure that their competent authorities have the power to: (a) Temporarily suspend or request a certification or authorisation body, or a court in accordance with national law, to temporarily suspend a certification or authorisation in respect of some or all of the relevant services provided or activities carried out by the essential entity; (b) Request that competent bodies or courts, in accordance with national law, temporarily prohibit any natural person with management responsibilities at executive director or legal representative level from exercising management functions in that essential entity. Temporary suspensions or prohibitions imposed in accordance with this paragraph shall only be applied until the entity concerned	arising from this Decree-Law and the respective applicable regulatory regime; b) Binding orders or instructions to adopt measures necessary to prevent, deter, or correct an incident, determining the time limits for their execution and reporting; c) Binding orders or instructions to remedy deficiencies or vulnerabilities; d) Binding orders or instructions for the purpose of complying

takes the necessary measures to remedy the deficiencies or comply with the requirements of the competent authority responsible for the implementation of those enforcement measures. The imposition of such temporary suspensions or prohibitions should be subject to appropriate procedural safeguards, in accordance with the general principles of Union law and the Charter, such as the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence. The implementing measures provided for in this paragraph shall not apply to the public administration entities covered by this Directive. 6. Member States shall ensure that any natural person responsible for an essential entity or acting as its legal representative, on the basis of the power to represent it,	with the provisions of Article 26 et seq. or, in the case of a relevant public entity, the provisions of Article 33, or to comply with the provisions of Article 40 et seq.; e) Orders for the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities potentially affected by a significant cyber threat of the nature of that threat, as well as

the authority to take decisions on its behalf or the authority to exercise control over it, has the power to ensure compliance with this Directive. Member States shall ensure that those natural persons can be held liable for the breach of their duties to ensure compliance with this Directive. As regards public administration entities, this paragraph shall apply without prejudice to national law on the liability of public officials and elected or appointed officials. 7. When taking any of the implementing measures referred to in (4) or (5), competent authorities shall respect the rights of the defence and consider the circumstances of each individual case and, as a minimum, take due account of:	of any protective or remedial measures that may be taken in response to that cyber threat; f) Orders for the entity concerned to implement, within a reasonable period of time, the recommendations made as a result of a security audit; g) The designation of a supervisor with appropriately circumscribed functions, for a limited period of time, to supervise the

Draft Law No .....

(a) The seriousness of the infringement and the importance of the provisions infringed, and in any event the following infringements shall be regarded as serious infringements: (i) Repeated violations, (ii) Non-notification or non-correction of significant incidents, (iii) Failure to remedy deficiencies following binding instructions from competent authorities; (iv) Obstruction of audits or follow-up activities ordered by the competent authority following the finding of an infringement; (v) Provision of false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations set out in	compliance of the entity concerned with the obligations laid down in Articles 26 et seq. and Article 40 et seq.; h) Orders for the entity concerned to publicise the aspects of infringements of this Decree-Law in a specific manner; 2 - In the event of non-compliance by any essential entity with the measures referred to in points (a) to (d) and (f) within the period determined by the competent cybersecurity authority, the competent

Draft Law No .....

(b) The duration of the infringement;	cybersecurity authority may, to the extent strictly necessary:
(c) Any previous relevant infringements by the entity concerned;	a) Suspend a certification, authorisation or licence for some or all of the relevant services provided or activities performed by the entity, or order a certification body to suspend it;
(d) Any material or immaterial damage caused, including any financial or economic loss, the effects on other services and the number of users affected;	b) Request the competent body to suspend the authorisation or licence for some or all of the relevant services provided or activities carried out by the entity;
(e) Any intention or negligence on the part of the infringer;	3 - The temporary
(f) Any measures taken by the entity to prevent or mitigate material or immaterial damage;	
(g) Any adherence to approved codes of conduct or certification mechanisms;	

(h) The level of cooperation of the natural or legal persons held responsible with the competent authorities. 8. Competent authorities shall provide a detailed statement of reasons for their decisions to apply implementing measures. Before taking such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow those entities a reasonable period of time to submit their comments, except in duly justified cases where immediate action to prevent or respond to incidents would otherwise be prevented. 9. Member States shall ensure that their competent authorities under this Directive inform the competent authorities in the same Member State under Directive (EU) 2022/2557 in the exercise of their	suspensions or disqualifications referred to in the previous paragraph shall continue until such time as the entity remedies the deficiencies or complies with the measures referred to in (1). 4 - The measures referred to in (2) shall not apply to public entities covered by this Decree-Law, without prejudice to the exercise of management and supervisory powers, in general terms. Article 57 Blocking and redirection measures 1 - The competent cybersecurity authority

Draft Law No .....

supervisory and enforcement powers aimed at ensuring compliance with this Directive by an entity identified as critical under Directive 2022/2557. Where appropriate, competent authorities under Directive (EU) 2022/2557 may request competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557. 10. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Supervisory Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 in the exercise of its supervisory and enforcement powers to ensure	may issue orders or instructions to counteract a cyber threat, cyber attack or incident to the network and information systems of the relevant essential, important or public entities resulting from the misuse of domain names or IP protocol addresses, in accordance with the following paragraphs. 2 - The types of abuse referred to in the preceding paragraph include, in particular: a) Distributed Denial of Service (DDoS) attacks; b) Malicious servers (Command and Control); c) Infected equipment

compliance with this Directive by an essential entity that is identified as a critical ICT third-party service provider pursuant to Article 31 Regulation (EU) 2022/2554.	(communication with Command and Control); d) Distribution of malicious code; e) Illegitimate use of a third party's name; f) Unsolicited emails (SPAM). 3 - To the extent strictly necessary to stop the misuse of domain names, the competent cybersecurity authority may order, in a duly reasoned manner: a) The registration of TLD names, requesting the holder of a domain name registration to take appropriate measures, within

Draft Law No .....

	a specified timeframe, to repress a cyber threat or respond to a cyber attack or incident; b) The registration of TLD names or DNS service providers, the blocking or redirection of domain names to a secure CNCS server, where they are manifestly dedicated to or involved in cyber-attacks or incidents and no other effective means are available to bring the cyber-attack or incident to an

Draft Law No .....

	end. 4 - In order to stop the misuse of IP protocol addresses, the CNCS may order undertakings providing electronic communications networks and services to block or redirect a dynamic or static IP protocol address to a secure CNCS server where those addresses are manifestly dedicated to or involved in the types of cyber-attacks or incidents referred to in (2)(a) to (d). 5 - The measures referred to in (3) and (4) shall not exceed the period of 60 days, which may be renewed for the same period

	where there is a strong likelihood, as assessed by a reasoned assessment, that cyber-attacks or incidents originating from the same addresses will persist or be resumed. 6 - The provisions of this Article shall also apply to providers of domain name registration services. Article 60 Cooperation in the field of critical infrastructure security 3 - Where the CNCS, the sectoral national cybersecurity authorities or the special national cybersecurity authorities, as the case may be, exercise their

Draft Law No .....

	supervisory powers in respect of an entity referred to in Article 3(5), they shall inform the competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December. 4 - Competent authorities resulting from the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December may, where necessary, request that the CNCS, the national sectoral cybersecurity authorities or the national special cybersecurity authorities, as

Draft Law No .....

	applicable, exercise their supervisory powers, in relation to an entity referred to in Article 3(5).
Article 33 Supervisory and enforcement measures in respect of important entities 1. Where they are presented with evidence, indications or information that an important entity is allegedly not complying with this Directive, in particular with Articles 21 and 23 thereof, Member States shall ensure that competent authorities act accordingly, where necessary, by taking supervisory *ex post* measures. Member States shall ensure that these measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	Article 53 Principles 1 - The competent cybersecurity authority, as the supervisory and enforcement authority, shall monitor and supervise compliance with this Decree-Law and take the necessary measures to ensure such compliance. 2 - Supervisory and enforcement activities shall be guided, *inter alia*, by the principles of public interest, legality, efficiency, effectiveness and proportionality and shall minimise, where

2. Member States shall ensure that, when carrying out their supervisory tasks in relation to important entities, competent authorities have the power to subject such entities to at least: (a) On-site inspections and *ex post* supervision remotely carried out by qualified professionals; (b) Specific security audits carried out by an independent body or a competent authority; (c) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate in cooperation with the entity concerned;	possible, their impact on the public, social and business activities of the supervised entities. 3 - Supervisory activity shall be based on risk assessment methodologies and, on the basis of that assessment and the principles referred to in the preceding paragraph, may determine the priority allocation of resources and the measures to be taken in accordance with the risk matrix applicable to the entity concerned, in particular as regards the conduct, frequency or type of on-site inspections, specific security audits or security checks and the type of information

(d) Requests for information necessary to assess *ex post* the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;	to be requested. 4 - Supervisory and enforcement activities shall be carried out with operational autonomy, including those targeting the relevant public entities. 5 - Supervisory and enforcement activities shall respect the legal and constitutional guarantees of individuals.
(e) Requests for access to data, documents and any information necessary for the performance of its supervisory tasks;	Article 55 Supervisory measures concerning relevant important and public entities 1 - Where the competent cybersecurity authority obtains evidence, indications or information that a
(f) Requests for evidence of the implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and their underlying evidence. The specific security audits referred to in point (b) of the first subparagraph shall be based on	

risk assessments carried out by the competent authority or the audited entity, or other available risk-related information. The results of the specific security audits shall be made available to the competent authority. The costs of specific security audits carried out by an independent body shall be paid by the audited entity, except in duly justified cases where the competent authority decides otherwise. 3. When exercising their powers under (2)(d), (e) or (f), the competent authorities shall indicate the purpose of the request and specify the information requested. 4. Member States shall ensure that, in the exercise of their enforcement powers in relation to important entities, competent authorities have powers to at least:	relevant important or public entity is not complying with this Decree-Law, it shall apply supervisory *ex post* measures provided for in the following paragraphs. 2 - The competent cybersecurity authority shall have the power to subject important entities to the following measures: a) On-site inspections and remote *ex post* supervision carried out by qualified professionals; b) Targeted security audits carried out by the competent authority itself or, where appropriate, by an entity appropriately

Draft Law No .....

(a) Issue warnings about infringements of this Directive by the entities concerned; (b) Adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies or infringements of this Directive; (c) Order those entities to cease conduct that infringes to submit a directive and to refrain from repeating such conduct; (d) Order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or comply with the notification obligations set out in Article 23 in a specified manner and within a specified period;	qualified for that purpose and offering guarantees of independence; c) Ad-hoc audits, in particular on the basis of the verification of a significant incident, non-compliance by the competent cybersecurity authority or infringement of this Decree-Law by the entity concerned; d) Security checks based on objective, non-discriminatory, fair and transparent risk assessment criteria, where appropriate in cooperation with the entity concerned; e) Requests for

Draft Law No .....

(e) Order the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities that are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures that may be taken by those natural or legal persons in response to that threat;	information necessary to assess compliance with the cybersecurity measures referred to in Articles 27 et seq. adopted by the entity concerned; f) Requests for access to data, documents and any information necessary for the performance of its supervisory tasks; g) Requests to provide evidence demonstrating the implementation of cybersecurity policies and procedures. 3 - The targeted audits referred to in (2) (b) shall be based on the risk analysis carried out by the competent
(f) Order the entities concerned to implement, within a reasonable period of time, the recommendations made as a result of a security audit;	
(g) Order those entities to make public the aspects of infringements of this Directive in a specified manner;	

Draft Law No .....

(h) Impose or request the imposition by the competent bodies or courts, in accordance with national law, of an administrative fine pursuant to Article 34, in addition to any of the measures referred to in points (a) to (g) of this paragraph. 5. Article 32(6), (7) and (8), apply *mutatis mutandis* the supervisory and enforcement measures provided for in this Article in respect of important entities. 6. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Supervisory Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 in the exercise of its supervisory	cybersecurity authority, the risk analysis carried out by the audited entity or other available risk-related information, including those contained in the technical harmonisation instructions and risk matrices prepared by the CNCS pursuant to Article 26(3), as well as the orders, instructions and guidelines of the competent cybersecurity authority. 4 - The costs of the targeted audits referred to in (2)(b) shall be borne by the audited entity, unless a reasoned decision to the contrary is taken by the competent cybersecurity authority. 5 - Requests for

and enforcement powers to ensure compliance with this Directive by an important entity that is identified as a critical ICT third-party service provider pursuant to Article 31 Regulation (EU) 2022/2554.	information and evidence referred to in (2)(e) to (g) shall indicate their purpose, specify the information requested, and set an appropriate and reasonable time limit for the essential entity to respond. Article 56 Implementing measures 1 - The competent cybersecurity authority may, in relation to relevant essential, important and public entities, take the following measures: a) Warnings of breaches of the obligations arising from this Decree-Law and the respective

	applicable regulatory regime; b) Binding orders or instructions to adopt measures necessary to prevent, deter, or correct an incident, determining the time limits for their execution and reporting; c) Binding orders or instructions to remedy deficiencies or vulnerabilities; d) Binding orders or instructions for the purpose of complying with the provisions of Article 26 et seq.

	or, in the case of a relevant public entity, the provisions of Article 33, or to comply with the provisions of Article 40 et seq.;
	e) Orders for the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities potentially affected by a significant cyber threat of the nature of that threat, as well as of any protective or remedial measures that

	may be taken in response to that cyber threat; f) Orders for the entity concerned to implement, within a reasonable period of time, the recommendations made as a result of a security audit; g) The designation of a supervisor with appropriately circumscribed functions, for a limited period of time, to supervise the compliance of the entity concerned with

Draft Law No .....

	the obligations laid down in Articles 26 et seq. and Article 40 et seq.; h) Orders for the entity concerned to publicise the aspects of infringements of this Decree-Law in a specific manner; i) The imposition of fines in accordance with the following Chapter. 2 - In the event of non-compliance by any essential entity with the measures referred to in points (a) to (d) and (f) within the period determined by the competent

	cybersecurity authority, the competent cybersecurity authority may, to the extent strictly necessary: a) Suspend, or order a certification body to suspend, a certification, authorisation or licence for some or all of the relevant services or activities performed by the organisation; b) Request the competent body to suspend the authorisation or licence for some or all of the relevant services provided or activities carried out by the entity;

Draft Law No .....

	3 - The temporary suspensions or disqualifications referred to in the previous paragraph shall continue until such time as the entity remedies the deficiencies or complies with the measures referred to in (1). 4 - The measures referred to in (2) shall not apply to public entities covered by this Decree-Law, without prejudice to the exercise of management and supervisory powers, in general terms.
Article 34 General conditions for imposing fines on essential and important	Article 61 Very serious administrative

Draft Law No .....

entities 1. Member States shall ensure that the imposition of fines on essential and important entities in accordance with this Article in respect of infringements of this Directive is effective, proportionate and dissuasive, taking into account the circumstances of each individual case. 2. Fines shall be imposed in addition to any of the measures referred to in Article 32(4)(a) to (h), Article 32(5) and Article 33(4) (a) to (g). 3. When deciding on the imposition of a fine and its amount in each individual case, due account shall be taken, as a minimum, of the elements set out in Article 32(7). 4. Member States shall ensure that, where they breach the obligations laid down in Article 21 or 23, essential entities are subject, in accordance with (2) and	offences 1 - The following shall constitute very serious administrative offences under this Decree-Law: a) Failure to comply with the decisions of the member of government responsible for cybersecurity, as provided for in Article 18(3); b) Failure to comply with the duty to adopt cybersecurity measures pursuant to Articles 27 to 29; c) Failure to comply with the obligations laid down in Article 30; d) Failure to comply with the obligations laid down in Article

(3) of this Article, fines of a maximum amount of not less than EUR 10 000 000 or of not less than 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher. 5. Member States shall ensure that, where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1.4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher. 6. Member States may provide for the power to impose periodic penalty payments to compel an essential or important entity to cease an infringement of this	31; e) Failure to comply with the obligations laid down in Article 32; f) Failure to comply with the duty to adopt the cybersecurity measures established by the CNCS pursuant to Article 33; g) Failure to comply with the obligations laid down in Article 34; h) Failure to comply with the obligations laid down in Article 36(1) and (2); i) Failure to comply with the obligations laid down in Article 37;

Draft Law No .....

Directive in accordance with a prior decision of the competent authority. 7. Without prejudice to the powers of the competent authorities under Articles 32 and 33, Member States may adopt rules to determine whether and to what extent administrative fines may be imposed on public administration entities. 8. Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article can be applied in such a way that the financial penalty is proposed by the competent supervisory authority and imposed by the competent national courts, while ensuring that these legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the financial penalties	j) Failure to comply with the notification obligation pursuant to Articles 40 to 44; k) Failure to comply with the obligation to report in accordance with Article 48; 2 - The administrative offences referred to in the preceding paragraph shall be punishable by the following fines: a) In the case of an essential entity: i) From EUR 2 500.00 to EUR 10 000 000.00 or 2 % of the total worldwide annual turnover of

imposed shall be effective, proportionate and dissuasive. The Member State shall notify the provisions it adopts pursuant to this paragraph to the Commission by 17 October 2024 and shall notify it without delay of any subsequent amendment affecting them.	the essential entity concerned in the preceding financial year, whichever is higher, if carried out by a legal person; ii) From EUR 500.00 to EUR 250 000.00 if committed by a natural person. b) In the case of an important entity: i) from EUR 1 750.00 to EUR 7 000 000.00 or

Draft Law No .....

	for a maximum amount which shall not be less than 1.4 % of the total worldwide annual turnover of the essential entity concerned in the preceding financial year, whichever is higher, if carried out by a legal person; ii) From EUR 500.00 to EUR 250 000.00 if

Draft Law No .....

	committed by a natural person. c) in the case of a relevant public entity included in Group A referred to in Article 7(2): i) From EUR 20 000.00 to EUR 5 000 000.00 if committed by a legal person; ii) From EUR 750.00 to EUR 20 000.00, if committed by a natural person. d) In the case of a relevant public entity included in

Draft Law No .....

	Group B as referred to in Article 7(3): i) From EUR 10 000.00 to EUR 450 000.00 if committed by a legal person; ii) From EUR 750.00 to EUR 20 000.00, if committed by a natural person. Article 62. Serious administrative offences 1 - The following shall constitute serious infringements under this Decree-Law: a) Failure to comply

	with the obligations laid down in Article 8; b) Failure to comply with the obligations laid down in Article 35; c) Failure to comply with the obligations laid down in Article 36(4) and (5); d) Failure to comply with the obligations laid down in Article 46; e) Failure to comply with the obligation laid down in Article 51(2); f) Failure to comply with the immediate enforcement measure provided for in Article 52(3); g) Failure to comply

	with binding warnings, orders or instructions issued by the competent cybersecurity authority under Article 56(1)(a) to (h); h) Breach of the suspension determined pursuant to Article 56(2)(a); i) Breach of the suspension determined pursuant to Article 56(2)(b); j) Failure to comply with the orders or instructions provided for in Article 57; 2 - The administrative offences referred to in the preceding paragraph shall be punishable by the following fines:

	a) in the case of an essential entity: i) from EUR 1 250.00 to EUR 5 000 000.00 or 1 % of the total worldwide annual turnover of the relevant essential entity in the preceding financial year, whichever is higher, if carried out by a legal person; ii) From EUR 250.00 to EUR 125 000.00 if

	committed by a natural person. b) In the case of an important entity: i) from EUR 875.00 to EUR 3 500 000.00 or for a maximum amount which shall not be less than 0.7 % of the total worldwide annual turnover of the essential entity concerned in the preceding financial

Draft Law No .....

	year, whichever is higher, if carried out by a legal person; ii) From EUR 250.00 to EUR 125 000.00 if committed by a natural person. c) In the case of a relevant public entity falling within 'Group A' as referred to in Article 7(2): i) From EUR 10 000.00 to EUR 2 500 000.00 if committed by a legal person;

Draft Law No .....

	ii) From EUR 375.00 to EUR 10 000.00 if committed by a natural person. d) In the case of a relevant public entity belonging to 'Group B' as referred to in Article 7(3): i) From EUR 5 000.00 to EUR 225 000.00 if committed by a legal person; ii) From EUR 375.00 to EUR 10 000.00 if committed by a natural person.

Draft Law No .....

	Article 66 Fixing the amount of the fine 1 - The specific fine is determined on the basis of the seriousness of the specific unlawfulness of the act, the fault of the agent, his economic situation and the economic benefit which he derived from the commission of the administrative offence. 2 - In determining the specific unlawfulness of the act and the fault of the agent, the following circumstances shall be taken into account: a) The seriousness of the infringement; b) The duration of the

Draft Law No .....

	infringement; c) The occasional or repeated nature of the infringement; d) The damage caused, including any financial or economic loss, the effects on other services and the number of users affected; e) The measures taken by the entity to prevent or mitigate the damage referred to in the previous subparagraph; f) The level of cooperation of the responsible natural or legal persons with the competent cybersecurity authority. 3 - For the purposes

	of point (a) of the preceding paragraph, the following shall be presumed to be serious: a) Repeated breaches of this Decree-Law; b) Failure to notify incidents pursuant to Articles 40 et seq.; c) Failure to correct significant incidents; d) The absence of correction of deficiencies following binding instructions from the competent authorities; e) Obstruction of audits or follow-up activities ordered by the competent cybersecurity authority, following the verification of an infringement of this

Draft Law No .....

	Decree-Law; f) The provision of false or grossly inaccurate information in relation to cybersecurity measures and obligations in relation to cybersecurity measures pursuant to Articles 27 et seq. or notification obligations pursuant to Articles 40 et seq. 4 - The provisions of point (f) of the preceding paragraph shall be without prejudice to liability under the Criminal Code. 5 - Except in case of intent, the initiation of administrative offence

	proceedings depends on prior warning of the agent, by the competent cybersecurity authority, to comply with the omitted obligation or reinstatement of the breached prohibition within a reasonable time. Article 67 Ancillary sanctions and other determinations Where justified by the seriousness of the infringement and the fault of the infringer, the competent cybersecurity authority may determine, at the same time as the fine: a) Publication in the Diário da República (Portuguese Official Gazette) and in one

	of the most widely circulated national, regional or local newspapers, depending on the relevant geographic market, at the offender's expense, of an extract from the conviction decision or, at least, the operative part of the conviction decision issued in the context of proceedings initiated under this Decree-Law, after it has acquired the force of res judicata; b) The prohibition of participation in public procurement procedures, where applicable; c) The adoption and

Draft Law No .....

	implementation of a cybersecurity training plan, to be implemented within six months; d) The adoption or amendment of a security plan, to be implemented within six months; e) Suspension of the provision of the service until the fulfilment of the omitted duties; f) Temporary disqualification of the holders of the management, direction and administrative bodies from performing their duties. Article 68

Draft Law No .....

	Compulsory penalties 1 - The addressees of a decision of the competent cybersecurity authority shall be subject to the payment of a sum of money for each day of delay in compliance, counted from the date of its notification. 2 - For the purposes of the preceding paragraph, the imposition on the agent of the payment of a pecuniary amount for each day of non-compliance that occurs beyond the deadline set for compliance with the obligation shall be considered a periodic penalty payment. 3 - The periodic penalty payment shall

	be set in accordance with criteria of reasonableness and proportionality, the daily amount of the penalty provided for in the preceding paragraph being set at EUR 500.00 when committed by a legal person and at EUR 100.00 when committed by a natural person. 4 - The daily amounts fixed may be increased for each day of non-compliance and may in no case exceed the maximum duration of 30 days.
Article 35 Offences involving a personal data breach 1. Where the competent authorities become aware, in the	Article 79 Personal data breach 1 - Where the competent cybersecurity authority

Draft Law No .....

course of supervisory or enforcement action, that the obligations laid down in Articles 21 and 23 of this Directive have been violated by an essential or important entity may result in a personal data breach within the meaning of Article 4(12), of Regulation (EU) 2016/679, which shall be notified pursuant to Article 33 of that Regulation shall, without undue delay, inform the supervisory authorities referred to in Articles 55 and 56 of that Regulation. 2. The supervisory authorities referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), the competent authorities shall not impose a fine pursuant to Article 34(2)(i) of that Regulation, for an offence referred to in (1) of this resulting from the same conduct as that which was the subject of the fine pursuant to Article 58(2)(i)of Regulation (EU)	becomes aware, in the course of supervisory action or enforcement action, that an infringement by an essential or important entity of the obligations laid down in Articles 27 to 29 and Articles 40 to 43 may lead to a personal data breach pursuant to Article 4(12) GDPR, which must be notified pursuant to Article 33 GDPR, it shall, without undue delay, inform the CNPD. 2 - In the event that the CNPD imposes an administrative fine pursuant to Article 58(2)(i) of the GDPR and other applicable national law, the competent cybersecurity authority

2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4)(a) to (h), Article 32(5) and in Article 33(4)(a) to (g) of this Directive. 3. Where the supervisory authority competent under Regulation (EU) 2016/679 is established in a Member State other than that of the competent authority, the latter shall inform the supervisory authority established in its own Member State about the possible personal data breach referred to in (1).	shall be prevented from imposing an administrative fine as a result of the commission of the same infringement pursuant to this Decree-Law, without prejudice to the provisions of the following paragraph. 3 - The competent cybersecurity authority may impose the implementing measures provided for in Article 56(1)(a) to (h) on essential and important entities whose breach of the obligations under this Decree-Law results in a personal data breach incident.
Article 36 Penalty Member States shall lay down the	N/A

rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.	
Article 37 Mutual assistance 1. Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with	Article 5 Extraterritorial scope 1 - In order to prevent significant cyber threats to the security of network and information systems of a large number of users, the CNCS may, after consulting the Supreme Cybersecurity

each other and assist each other as necessary. Such cooperation shall entail at least that: (a) The competent authorities applying supervisory or enforcement measures in a Member State inform and consult, through the Single Point of Contact, the competent authorities of the other Member States concerned about the supervisory and enforcement measures taken; (b) A competent authority may request another competent authority to take supervisory or enforcement measures;	Council, adopt corrective or restrictive enforcement measures, including the order to suspend the service in the national territory, addressed to a service provider without establishment or representation in the national territory that does not offer appropriate cybersecurity measures. 2 - Except where the measures are urgent, the CNCS shall provide a preliminary statement of reasons for the decisions to the service provider, granting a time limit for reply of no less than 10 days. 3 - For the purposes of determining and

(c) A competent authority, upon receiving a reasoned request from another competent authority, shall provide the same mutual assistance, proportionate to the resources at its disposal, so that supervisory or enforcement measures can be carried out in an effective, efficient and consistent manner. Mutual assistance referred to in point (c) of the first subparagraph may cover information requests and supervisory measures, including requests to conduct on-site inspections, off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse such a request, unless it is determined that it is not competent to provide the assistance requested, that the assistance requested is not proportionate to the supervisory tasks of the competent authority, or that the request concerns	substantiating the implementing measures provided for in the preceding paragraphs, the CNCS shall take into account the actions and measures, as well as their effectiveness and extent, taken by European and international cybersecurity authorities. 4 - The competent cybersecurity authority, in accordance with its competences and to the extent necessary, may, in relation to an entity with a relevant connection to the national territory, assist the competent authorities of the Member States of the European Union, upon their reasoned request,

information or engages in activities which, if disclosed or carried out, would be contrary to the essential interests of national security, public security or defence of the Member State. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, at the request of one of the Member States concerned, the Commission and ENISA. 2. Where appropriate and by mutual agreement, the competent authorities of different Member States may carry out joint supervisory actions.	in particular by: d) Providing information regarding a supervisory or enforcement measure taken in relation to that entity through its Single Point of Contact; e) The application of supervisory or enforcement measures in accordance with Chapter VI, where necessary together with the competent authority of the respective Member State of the European Union; f) Providing support to the competent authority of the respective Member

Draft Law No .....

	State of the European Union with regard to the application by the latter of supervisory or enforcement measures, which may include the forms of assistance referred to in the previous points. 5 - The competent cybersecurity authority may refuse the assistance requested in accordance with the preceding paragraph only if it exceeds its powers, is disproportionate to its supervisory functions or compromises essential interests of the Portuguese State in terms of national security, public security

Draft Law No .....

	or defence.
Article 38 Exercise of the delegation 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article- 2. The power to adopt delegated acts referred to in Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023. 3. the delegation of power referred to in Article 24(2) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision- It shall take effect on the day following that of its publication in the *Official Journal of the European Union* or a later date specified therein. It shall not affect the validity of any delegated acts	N/A

already in force. 4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making- 5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. 6. Delegated acts adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at	

the initiative of the European Parliament or of the Council.	
Article 39 Committee procedure 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or one of its members so requests.	N/A
Article 40 Assessment	N/A

By 17 October 2027, and every 36 months thereafter, the Commission shall evaluate the application of this Directive and submit a report to the European Parliament and to the Council. The report shall assess, in particular, the relevance of the size of the entities concerned and of the sectors, subsectors and types of entities referred to in Annexes I and II for the functioning of the economy and society with regard to cybersecurity. For that purpose, and in order to promote strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs Network on the experience gained at strategic and operational level. The report shall be accompanied, if appropriate, by a legislative proposal.	
Article 41 Transposition	N/A

Draft Law No .....

1. Member States shall adopt and publish, by 17 October 2024 at the latest, the provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof- They shall apply those provisions from 18 October 2024. 2. The provisions adopted by the Member States referred to in (1) shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	
Article 42 Amendments to Regulation (EU) No 910/2014 In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024.	N/A
Article 43	N/A

Draft Law No .....

Amendments to Directive (EU) 2018/1972 In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024. *Article 44* Repeal Directive (EU) 2016/1148 is repealed with effect from 18 October 2024. References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex III.	
Article 45 Entering into force This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.	N/A
Article 46	N/A

PRESIDENCY OF THE COUNCIL OF MINISTERS

Draft Law No .....

Target audience This Directive is addressed to the Member States.	