GENERAL SERIES

Shipping abb. post. 45% - art. 2, paragraph 20/ b
Law 23-12-1996, n. 662 - Rome Branch
Law 27-02-2004, n. 46 - Rome Branch

Year 165 - Number 230

OFFICIAL JOURNAL

OF THE ITALIAN REPUBLIC

PART ONE

DAY Rome - Tuesday, October 1, 2024

PUBLISHED EVERY NON-HOLIDAYS

DIRECTION AND EDITORIAL OFFICE AT THE MINISTRY OF JUSTICE - OFFICE FOR PUBLICATION OF LAWS AND DECREES - VIA ARENULA 70 - 00186 ROME
ADMINISTRATION AT THE STATE PRINTING INSTITUTE AND MINT - VIA SALARIA, 691 - 00138 ROME - SWITCHBOARD 06-85081 - STATE BOOKSTORE ADMINISTRATION AT THE STATE PRINTING INSTITUTE AND MINT - STATE BOOKSTORE - PIAZZA G. VERDI 10 - 00198 ROME - SWITCHBOARD 06-85081
PIAZZA G. VERDI, 1 - 00198 ROME

The **Official Journal, Part One,** in addition to the **General Series,** publishes five special Series, each distinguished from autonomous numbering:

1st Special Series: Constitutional Court (published on Wednesday)
2nd Special Series: European Union (published on Mondays and Thursdays)
3rd Special Series: Regions (published on Saturdays)
4th Special Series: Competitions and Exams (published on Tuesdays and Fridays)
5th Special Series: Public Contracts (published on Mondays, Wednesdays, and Fridays)

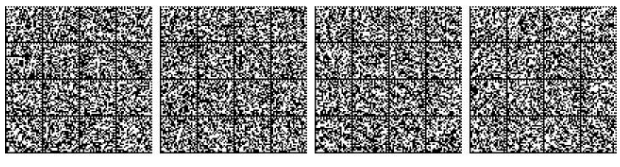
The **Official Journal, Part Two,** "Advertisement Sheet", is published on Tuesdays, Thursdays and Saturdays

NOTICE TO THE ADMINISTRATIONS

In order to optimize the procedure for publishing documents in the Official Journal, the Administrations Please send, simultaneously and in parallel with the paper transmission, as per the regulations, an electronic copy of the same (in Word format) to the following certified email address: gazzettaufficiale@giustiziacert.it, ensuring that the details of the electronic transmission (sender, subject and date) are clearly indicated in the paper transmission note.

If you do not yet have a certified email (PEC), and until it is adopted, you can send documents to: gazzettaufficiale@giustizia.it

SUMMARY



LAWS AND OTHER REGULATORY ACTS

DECREE-LAW 1 October 2024 , n. **137 .**

Urgent measures to combat violence against healthcare, social healthcare, auxiliary, and care professionals in the performance of their duties, as well as damage to healthcare assets.

THE PRESIDENT OF THE REPUBLIC

Having regard to Articles 77 and 87, fifth paragraph, of the Constitution;

Having seen Law No. 400 of 23 August 1988, concerning "Regulation of Government Activity and Organization of the Presidency of the Council of Ministers" and, in particular, Article 15;

Having seen Law No. 113 of 14 August 2020, containing "Provisions regarding safety for healthcare and social healthcare professionals in the exercise of their duties";

Having seen Legislative Decree No. 34 of March 30, 2023, converted, with amendments, by Law No. 56 of May 26, 2023, containing "Urgent measures to support families and businesses in the purchase of electricity and natural gas, as well as in matters of health and tax compliance" and, in particular, Article 16, which provides provisions on combating acts of violence against healthcare workers;

Having seen Legislative Decree No. 31 of 19 March 2024, containing "Supplementary and corrective provisions of Legislative Decree No. 150 of 10 October 2022, implementing Law No. 134 of 27 September 2021, delegating the Government to ensure the efficiency of the criminal process, as well as restorative justice and provisions for the speedy resolution of judicial proceedings";

Given the extraordinary necessity and urgency, given the resurgence of serious episodes of violence against professionals and public health facilities, particularly in emergency rooms, to adopt suitable measures to establish a valid and effective deterrent and counteract such episodes, which affect and humiliate the personnel assigned to these delicate functions and risk impoverishing the public health system;

Having seen the resolution of the Council of Ministers, adopted at the meeting of 27 September 2024;

On the proposal of the President of the Council of Ministers, the Ministers of Health and Justice, in agreement with the Minister of the Interior;

EMANA
the following decree-law:

Art. 1.

Amendments to Article 635 of the Criminal Code

1. In Article 635 of the Criminal Code, after the second paragraph, the following is inserted:

Anyone who, within or on the premises of residential or semi-residential health or social-health facilities, whether public or private, through violence or threats, or in connection with the crime set forth in Article 583- *quater ,* destroys, disperses, deteriorates, or renders, in whole or in part, unusable property existing therein or in any case intended for the health or social-health service, shall be punished with imprisonment for one to five years and a fine of up to 10,000 euros. If the act is committed by several people working together, the penalty is increased.

Art. 2.

Amendments to Articles 380 and 382 -bis *of the Code of Criminal Procedure*

1. The following amendments are made to the Code of Criminal Procedure: *a)*

in Article 380, paragraph 2, after letter a- *bis)* the following are inserted: «a *-ter)* crime

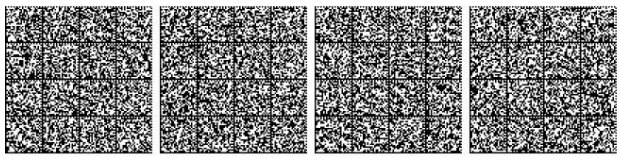
of personal injury to personnel practicing a health or social-health profession and to anyone who carries out auxiliary activities functional to it as provided for by Article 583 *-quater ,* second paragraph, of the Criminal Code; a *-quater)* crime of damage

as provided for by

from Article 635, third paragraph, of the Criminal Code;»; *b)* in

Article 382 *-bis ,* after paragraph 1 the following is added: «1 *-bis .* In cases

of non-negligent crimes for which arrest is provided for in flagrante delicto, committed within or on the premises of residential or semi-residential public or private health or social-health facilities, to the detriment of persons exercising a health or social-health profession in the exercise or because of the functions or service as well as anyone carrying out auxiliary care, health care or rescue activities, functional to the performance of said professions, in the exercise or because of such activities, or committed on things existing there or in any case intended for the health or social-health service, when it is not possible to proceed immediately to the arrest for reasons of public or individual safety or security or for reasons inherent to the regular provision of the service, anyone who, on the basis of video-photographic documentation or other documentation legitimately obtained from computer or telematic communication devices, from which it unequivocally emerges, is considered to be in a state of flagrante delicto pursuant to Article 382. the fact, the author is the one who results, provided that



the arrest is carried out no later than the time necessary for his identification and, in any case, within forty-eight hours of the event.».

Art. 3.

Financial invariance clause

1. Implementation of the provisions of this decree must not result in new or increased burdens on public finances. The administrations and authorities concerned shall carry out the activities set forth herein within the human, instrumental, and financial resources available under current legislation.

Art. 4.

Entry into force

1. This decree enters into force on the day following its publication in the *Official Journal* of the Italian Republic and will be submitted to the Chambers for conversion into law.

This decree, bearing the State seal, will be included in the Official Collection of Legislative Acts of the Italian Republic. All concerned are required to observe it and ensure its observance.

Given in Rome, this 1st day of October 2024

MATTARELLA

MELONI, *President of the Council of Ministers*

SCHILLACI, *Minister of Health*

NORDIO, *Minister of Justice*

PIANTEDOSI, *Minister of the Interior*

Seen, *the Keeper of the Seals:* NORDIO

24G00158

LEGISLATIVE DECREE 4 September 2024 , n. **138 .**

Transposition of Directive (EU) 2022/2555 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.

THE PRESIDENT OF THE REPUBLIC

Having regard to Articles 76 and 87, fifth paragraph, of the Constitution;

Having regard to Law No. 400 of 23 August 1988, concerning "Regulation of Government Activity and Organization of the Presidency of the Council of Ministers" and, in particular, Article 14;

Having regard to Law No. 234 of 24 December 2012, containing "General rules on Italy's participation in the formation and implementation of European Union legislation and policies" and, in particular, Articles 31 and 32; Having regard to Law No. 15 of 21

February 2024, containing "Delegation to the Government for the transposition of European directives and the implementation of other European Union legislative acts - European Delegation Law 2022-2023" and, in particular, Article 3; Having regard to Directive (EU) 2022/2555 of

the European Parliament and of the Council of 14 December 2022 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; Having regard to the Commission Communication of 13 September 2023 on the application of Article 4, paragraphs 1

and 2, of Directive (EU) 2022/2555; Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data

and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; Having regard to Regulation (EU) 2024/1183

of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European framework for a digital identity; Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council

of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 1095/2010; 526/2013 ('Cybersecurity Regulation'); Having regard to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises; Having regard to Directive 2013/40/EU of

the European Parliament and of the Council of 12 August 2013

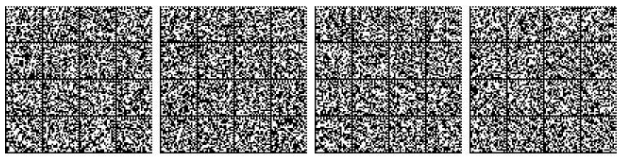
on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA; Having

regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No

1060/2009, (EU) No 648/2012, (EU) No 600/2014,

(EU) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 1060/2014, Having regard to Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards

digital operational resilience for the financial sector;



Having regard to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC; Having regard to Legislative

Decree no. 196 of 30 June 2003 containing the «Personal Data Protection Code, containing provisions for the adaptation of national legislation to Regulation (EU) no. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC»;

Having seen the legislative decree of 1 August 2003, n. 259, re-song «Electronic Communications Code»;

Having seen Legislative Decree No. 82 of 7 March 2005, containing the "Digital Administration Code" and, in particular, the provisions regarding the functions of AgID and IT security;

Having seen Legislative Decree No. 144 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005, containing «Urgent measures to combat international terrorism»; Having seen Law

No. 124 of 3 August 2007, containing «Information system for the security of the Republic and new rules on secrecy»; Having seen Legislative Decree No. 118

of 23 June 2011, containing «Provisions regarding the harmonization of accounting systems and budget formats of the Regions, local authorities and their bodies, pursuant to Articles 1 and 2 of Law No. 42 of 5 May 2009»;

Having seen Legislative Decree No. 83 of 22 June 2012, converted, with amendments, by Law No. 134 of 7 August 2012, containing "Urgent measures for the growth of the country" and, in particular, Article 19, which established the Agency for Digital Italy (AgID);

Having regard to Legislative Decree No. 39 of 4 March 2014, concerning the "Implementation of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, which replaces Framework Decision 2004/68/GAI"; Having regard to

Legislative Decree No. 174 of 30 October 2015, converted, with amendments, by Law No. 198 of 11 December 2015, concerning the "Extension of international missions of the Armed Forces and police, development cooperation initiatives and support for reconstruction processes and participation in the initiatives of international organisations for the consolidation of peace and stabilisation processes"; Having regard to Legislative Decree No. 18 May 2018, 65, implementing

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;

Having seen Legislative Decree No. 105 of 21 September 2019, converted, with amendments, by Law No. 133 of 18 November 2019, containing "Urgent provisions regarding the national cybersecurity perimeter";

Having seen the legislative decree of 14 June 2021, n. 82, converted, with amendments, by law of 4 August 2021, n. 109, containing «Urgent provisions on cybersecurity

Having regard to Law No. 90 of 28 June 2024, containing «Provisions on strengthening national cybersecurity and cybercrime»; Having regard to the

legislative decree adopted pursuant to Article 5 of Law No. 15 of 2024 for the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council

of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC; Having regard to the Prime Ministerial Decree No. 5 of 6 November 2015, containing «Provisions for the administrative protection of state secrets and classified and exclusively disseminated information», published in the *Official Journal* No. 284

of 5 December 2015;

Having seen the decree of the President of the Council of Ministers of 17 February 2017, concerning the "Directive containing guidelines for national cyber protection and IT security", published in the *Official Journal*
n. 87 of 13 April 2017;

Having heard the National Cybersecurity Agency, pursuant to Article 3 of Law No. 15 of 2024;

Having seen the preliminary resolution of the Council of ministers, adopted at the meeting of 10 June 2024;

Having acquired the opinion of the Unified Conference referred to in Article 8 of Legislative Decree No. 281 of 28 August 1997, issued in the session of 11 July 2024 Having acquired the

opinions of the competent Commissions of the Chamber of Deputies and the Senate of the Republic;

Having seen the resolution of the Council of Ministers, adopted at the meeting of 7 August 2024;

On the proposal of the President of the Council of Ministers and the Minister for European Affairs, the South, Cohesion Policies and the PNRR, in agreement with the Ministers for Public Administration, Foreign Affairs and International Cooperation, the Interior, Justice, Defence, Economy and Finance, Business and Made in Italy, Agriculture, Food Sovereignty and Forests, Environment and Energy Security, Infrastructure and Transport, Universities and Research, Culture and Health;

EMANA
the following legislative decree:

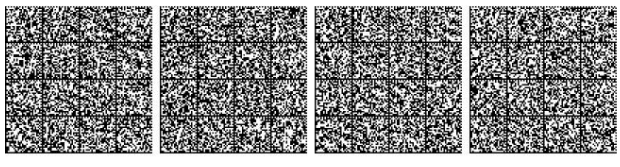
Chapter I

GENERAL PROVISIONS

Art. 1.

Object

1. This Decree establishes measures aimed at ensuring a high level of IT security at national level, contributing to increasing the common level of security in the European Union in order to improve the functioning of the internal market.



2. For the purposes of paragraph 1, this decree provides:

a) the National Cybersecurity Strategy, containing provisions aimed at ensuring a high level of cybersecurity;

b) the integration of the IT crisis management framework, within the context of the national organization for the management of crises involving cybersecurity aspects, referred to in Article 10 of Legislative Decree no. 82 of 4 June 2021, converted, with amendments, by Law no. 109 of 4 August 2021;

c) the confirmation of the National Cybersecurity Agency as:

1) Competent national authority NIS, regulating its powers relating to the implementation and enforcement of this decree;

2) NIS single point of contact, ensuring national and cross-border coordination;

3) National intervention group for cyber security in the event of an incident at national level

(CSIRT Italy);

d) the designation of the National Cybersecurity Agency, acting as coordinator pursuant to Article 9, paragraph 2, of Directive (EU) 2022/2555, and the Ministry of Defence, each for the areas of competence indicated in Article 2, paragraph 1, letter *g)* , as National Authorities for the management of large-scale cyber crises, ensuring consistency with the existing national framework for general cyber crisis management, without prejudice to the tasks of the Cybersecurity Unit referred to in Article 9 of Legislative Decree no. 82 of 14 June 2021; *e)* the identification of NIS sector authorities that collaborate with the National Cybersecurity Agency, supporting its functions as the competent National

NIS Authority and NIS Single Point of Contact;

f) the indication of the criteria for identifying the entities to which this decree applies and the definition of the related obligations regarding cybersecurity risk management measures and incident notification; *g)* the adoption of measures regarding cooperation and information

sharing for the purposes of applying this decree, in particular, through national participation at European Union level:

1) to the NIS Cooperation Group between NIS competent authorities and between single points of contact of the Member States of the European Union, with a view to increasing trust and cooperation at Union level;

2) the Cyber Crisis Liaison Organisations Network (EU-CyCLONe) to support the coordinated management of large-scale cyber incidents and crises at operational level and to ensure the regular exchange of relevant information between Member States and European Union institutions, bodies, offices and agencies;

3) to the national CSIRT network with a view to ensuring rapid and effective technical cooperation.

Art. 2.

Definitions

1. For the purposes of this decree, the following definitions apply:
a) "National

Cybersecurity Strategy": the coherent framework that provides for the strategic objectives and priorities in the field of cybersecurity, as well as the governance for their achievement, referred to in Article 9; *b)* "National Cybersecurity Agency": the

National Cybersecurity Agency referred to in Article 5, paragraph 1, of Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 109 of 4 August 2021;

c) "Cybersecurity Unit": the Cybersecurity Unit referred to in Article 8 of Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 109 of 4 August 2021; *d)* "Competent National Authority for NIS": the

National Cybersecurity Agency, as the competent National Authority for NIS referred to in Article 10, paragraph 1;

(e) 'NIS Single Point of Contact' means the National Cybersecurity Agency, as the Single Point of Contact
NIS referred to in Article 10, paragraph 2; *f)*

"NIS Sector Authority": the Administrations designated as Sector Authorities referred to in Article 11, paragraphs 1 and 2;

(g) "National cyber crisis management authorities": for the part relating to national resilience referred to in Article 1 of Legislative Decree No. 82 of 2021, the National Cybersecurity Agency, acting as coordinator pursuant to Article 9, paragraph 2, of Directive (EU) 2022/2555, and, for the part relating to State defence, the Ministry of Defence, as national authorities responsible for managing large-scale cybersecurity incidents and crises, referred to in Article 9 of Directive (EU) 2022/2555; *(h)* "National CSIRTs": the National Cybersecurity Incident Response Teams referred to in Article 10, paragraph 1, of Directive (EU)

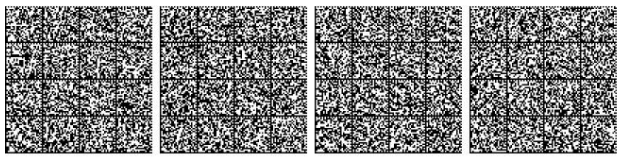
2022/2555 of the European Parliament and of the Council of 14 December 2022; *i)* «CSIRT Italia»: the National Cybersecurity Incident Response Group pursuant to Article 15, paragraph 1, operating within the National Cybersecurity Agency;

(l) 'NIS Cooperation Group' means the Cooperation Group referred to in Article 18, established pursuant to Article 14 of Directive (EU) 2022/2555;

(m) 'EU-CyCLONe' means the Network of Cyber Crisis Liaison Organisations referred to in Article 19, established pursuant to Article 16 of Directive (EU) 2022/2555; (n) 'National CSIRTs Network' means the

Network of National CSIRTs referred to in Article 20, established pursuant to Article 15 of Directive (EU) 2022/2555; *(o)* 'ENISA' means the European Union Agency

for Cybersecurity, as referred to in Article 3 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019;



p) "information and network system":

1) an electronic communications network pursuant to Article 2, paragraph 1, letter *vv) ,* of Legislative Decree no. 259 of 1 August 2003; 2) any device or group of

interconnected or linked devices, one or more of which perform, on the basis of a program, automatic processing of digital data; 3) digital data stored, processed, extracted or transmitted by means

of networks or devices referred to in numbers 1) and 2), for their operation, use, protection and maintenance; *q)* "security of information and network systems": the ability of information and network systems

to resist, with a given level of reliability, events that could compromise the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or of the services offered by such information and network systems or accessible through them;

r) "cybersecurity": the set of activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats, as defined in Article 2, point 1), of Regulation (EU) 2019/881; *s)* "cybersecurity": without prejudice to the definitions in letters *q)* and *r) ,* the set of activities referred to in Article 1, paragraph 1, letter *a) ,* of

Legislative Decree no. 82 of 14 June 2021, converted, with amendments, by Law no. 109 of 4 August 2021; *t)* "incident": an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by information and network systems or accessible through them; *u)*

"near-miss": so-called *near-miss* an event that could have led to an accident but which did not occur, including where the accident was effectively avoided;

,

(v) 'large-scale cybersecurity incident' means an incident that causes a level of disruption beyond the capacity of a Member State to respond to it or that has a significant impact on at least two Member States; *(z)* 'incident management' means the actions and procedures

aimed at preventing, detecting, analysing and containing or responding to and recovering from an incident; (aa) 'risk' means the combination of the magnitude of the impact of an

incident, in terms of damage or disruption, and the likelihood of its occurrence;

(bb) 'cyber threat' means any circumstance, event or action that may damage, disrupt or otherwise negatively impact information and network systems, the users of such systems and other persons, as defined in point (8) of Article 2 of Regulation (EU) 2019/881; *(cc)* 'significant cyber threat' means a cyber threat which, based on its technical characteristics, is

expected to have a serious impact on an entity's information and network systems or on the users of such systems.

services provided by a subject causing significant material or immaterial losses;

dd) "multi-risk approach": the so-called *all-hazards* approach , the approach to risk management that considers those deriving from all types of threats to information and network systems as well as to their physical context, such as theft, fire, flood, interruptions, even

partial, of telecommunications and electricity, and in general unauthorised physical access;

ee) "single points of failure": so-called *single points of failure ,* a single component of a system on which the functioning of the system itself depends;

(ff) 'ICT product' means an element or group of elements of an information or network system as defined in point (12) of Article 2 of Regulation (EU) 2019/881; *(gg)* 'ICT service' means a service consisting

wholly or mainly of the transmission, storage, retrieval or processing of information by means of information or network systems as defined in point (13) of Article 2 of Regulation (EU) 2019/881;

(hh) 'ICT process' means a set of activities carried out to design, develop, deliver or maintain an ICT product or ICT service as defined in point (14) of Article 2 of Regulation (EU) 2019/881; (ii) 'vulnerability' means a weakness, susceptibility or defect in ICT

products or ICT services that can be exploited by a cyber threat; (ll) '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 2012; *mm)* 'Internet exchange point' means *a so-called Internet exchange point* (IXP) which means a network infrastructure that enables the

interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of Internet traffic, which provides interconnection only to autonomous systems and which does not require Internet traffic passing between any pair of participating autonomous systems to pass through a third autonomous system or otherwise alter or interfere with such traffic; *nn)* 'Domain name system' means *a so-called domain name system* (DNS) which means a hierarchical and distributed name system that allows the identification of services and resources on the Internet,

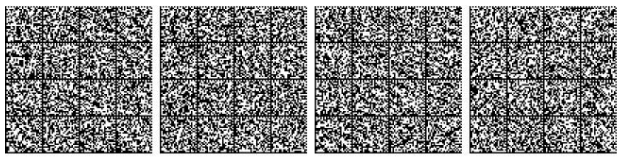
enabling end-user devices to use Internet routing and connectivity services in order to access those services and resources;

oo) «domain name system service provider nio»: a subject who alternatively provides:

1) publicly accessible recursive domain name resolution services for Internet end-users; 2) authoritative domain name

resolution services for use by third parties, with the exception of root name *servers ;*

pp) 'top-level domain name registry': the so-called TLD (top-*level domain)* name registry or *registry ,* an entity to which a specific top-level domain has been delegated and which is responsible



of the administration of that top-level domain, including the registration of domain names under that top-level domain, and of the technical operation of that top-level domain, including the operation of name servers, the maintenance of databases and the distribution of top-level domain zone files between name servers, whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where top-level domain names are used by a registry exclusively for its own use;

(qq) 'domain name registration service provider' means a *registrar* or an agent acting on behalf of *a registrar ,* such as a privacy registration service provider or reseller or proxy; *(rr)* 'digital service' means any information society service, that is to

say any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, as defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015; *(ss)* '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

2024; *(tt)* 'trust service provider' means a natural or legal person who provides one or more trust services, either as a qualified trust service provider or as a non-qualified trust service provider, as defined in point

(19) of Article 3 of Regulation (EU) No 910/2014; *(uu)* 'qualified trust service' means a trust service that meets the relevant requirements set out in Regulation (EU) No 910/2014, pursuant to point (17) of Article 3 thereof; *(vv)* 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services

and to whom the supervisory body assigns the status of qualified trust service provider, as defined in point (20) of Article 3 of Regulation (EU) No 910/2014; *(zz)* 'online marketplace' means a service using software, including websites,

parts of websites or an application, operated by or on behalf of the trader, which allows consumers to conclude distance contracts with other traders or consumers, as defined in Article 2(n) of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005; *(aaa)* 'online search engine' means a digital service that allows the user to ask

questions in order to search, in principle, all websites, or all websites in a particular language, based on a query on any topic in the form of a keyword, spoken query, phrase or other input, and that returns results in any format in which information relating to the requested content can be found, as defined in point (5) of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019;

(bbb) 'cloud computing service' means a digital service that enables on-demand administration of, and widespread remote access to, a scalable and elastic *pool* of shareable computing resources, even where those resources are distributed across multiple locations; (ccc) 'data center service' means a service

comprising facilities, or groups of facilities, dedicated to centrally hosting, interconnecting, and operating computing and network equipment that provides data storage, processing, and transport services, together with all facilities and infrastructure for energy distribution and environmental control;

ddd) 'content delivery network': a so-called *content delivery network* (CDN), a network of geographically distributed servers 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;

(eee) 'social networking service platform' means a platform that allows end-users to connect, share, discover and communicate with each other across multiple devices, in particular through chat, posts, videos and recommendations; *(fff)* 'public electronic communications network' means an electronic communications

network, used wholly or mainly for the provision of publicly available electronic communications services, which supports the transfer of information between network termination points, as defined in point (8) of Article 2 of Directive

(EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018; *(gg)*

'electronic communications service' means an electronic communications service as defined in point (4) of Article 2 of Directive (EU) 2018/1972; *(hhh)* 'entity' means a natural or legal person,

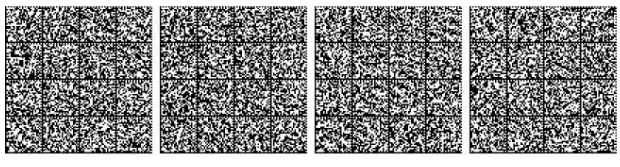
created and recognised as such in accordance with the national law applicable at its place of establishment, who may, acting in its own name, exercise rights and be subject to obligations; *(iii)* 'managed service provider' means an entity that provides services relating to the installation, management,

operation or maintenance of products, networks, infrastructures, ICT applications or any other information and network systems, through active assistance or administration carried out on the customers' premises or remotely;

(lll) 'managed security service provider' means a managed service provider that performs or provides support for activities related to the management of information security risks; *mmm)* 'research organisation'

means an entity whose primary objective is to conduct applied research or experimental development with a view to commercially exploiting the results of such research, but which does not include educational institutions;

nnn) "audit": a systematic, documented and independent verification activity, remote or on-site, aimed at assessing compliance with the obligations set out in Chapter IV of this decree, carried out by a qualified independent body or by the competent national NIS Authority.



Art. 3.

Scope of application

1. The scope of this decree includes the public and private entities of the types listed in Annexes I, II, III, and IV, which form an integral part of this decree, and which are subject to national jurisdiction pursuant to Article 5. Annexes I and II describe the sectors considered highly critical and critical, respectively, as well as the related subsectors and types of entities. Annexes III and IV describe, respectively, the categories of public administrations and the additional types of entities to which this decree applies.

2. This decree applies to entities of the types set out in Annexes I and II, which exceed the ceilings for small enterprises pursuant to Article 2, paragraph 2, of the Annex to Recommendation 2003/361/EC.

3. Article 3, paragraph 4, of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 does not apply for the purposes of this Decree.

4. In order to determine whether an entity is to be considered a medium-sized or large enterprise within the meaning of Article 2 of the Annex to Recommendation 2003/361/EC, Article 6, paragraph 2, of that Annex shall apply, unless this is proportionate, also taking into account the independence of the entity from its associated undertakings in terms of the information and network systems it uses in the provision of its services and in terms of the services it provides.

5. This decree also applies, regardless of their size, to:

a) to subjects who are identified as critical subjects pursuant to the legislative decree, which implements Directive (EU) 2022/2557 of the European Parliament and of the Council, of 14 December 2022;

(b) providers of public electronic communications networks or publicly available electronic communications services; *(c)* trust service providers; *(d)* top-level domain name registries and domain name system service providers; *(e)* domain name registration service providers.

6. This decree also applies, regardless of their size, to the public administrations referred to in Article 1, paragraph 3, of Law No. 196 of 31 December 2009, included in the categories listed in Annex III.

7. On the basis of a gradual approach, the evolution of the public administration's level of exposure to risk, the probability of incidents occurring and their severity, including their social and economic impact, also taking into account the criteria referred to in paragraph 9, further categories of public administrations to which this decree applies may be identified by one or more decrees of the President of the Council of Ministers adopted in accordance with the procedures referred to in Article 40, paragraph 2, in order to adapt the list of categories in Annex III.

8. This decree also applies, regardless of their size, to the types of entities listed in Annex IV, identified according to the procedures referred to in paragraph 13.

9. This decree also applies to entities in the sectors or types listed in Annexes I, II, III, and IV, regardless of their size, identified according to the procedures referred to in paragraph 13, if: *a)* the entity is identified before the date of entry into force of this decree as an operator of essential services pursuant to Legislative Decree no. 65 of 18 May 2018; *b)* the entity is the sole national provider of a service that is essential for the maintenance of fundamental social or economic activities; *c)* a disruption to the service provided by the entity could have a significant impact on public safety, public security, or public health;

(d) a disruption in the service provided by the entity could pose a significant systemic risk, particularly for sectors where such disruption could have a cross-border impact; (e) the entity is critical due to its particular importance at national or regional level for that particular sector or type of service or for other independent sectors within the territory of the State; *(f)* the entity is considered critical pursuant to this Decree as a systemic element of the supply chain, including digital, of one or more entities considered essential or important.

10. Finally, this decree applies, regardless of its size, to the company associated with an essential or important entity, if it satisfies at least one of the following criteria: *a)* it adopts decisions or exercises a dominant influence on decisions relating to the IT security risk management measures of an important or essential entity; *b)* it owns or manages information and network systems on which the provision of services of the important or essential entity depends;

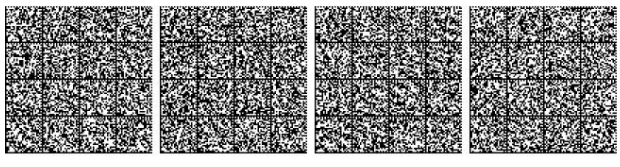
c) performs IT security operations of the important or essential subject;

d) provides ICT or security services, including managed services, to the important or essential entity.

11. The provisions on the protection of personal data pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Legislative Decree no. 196 of 30 June 2003, as well as on the fight against the sexual abuse and exploitation of minors and child pornography pursuant to Legislative Decree no. 39 of 4 March 2014, remain unchanged.

12. The competent national NIS Authority applies the safeguard clause referred to in paragraph 4, according to the determination criteria identified with the methods referred to in Article 40, paragraph 1.

13. The subjects referred to in paragraphs 8 and 9 are identified by the competent national NIS Authority, on proposal of the sector Authorities, according to the procedures set out in article



Article 40, paragraph 4. The competent national NIS Authority shall notify such entities of their identification for the purposes of registration referred to in Article 7, paragraph 1.

14. The provisions of Article 17 and Chapters IV and V of this decree do not apply to entities identified as essential or important in sectors 3 and 4 of Annex I, to which the provisions of Regulation (EU) 2022/2554 apply.

15. Pursuant to Article 2, paragraph 10, of the Directive, this decree does not apply to entities exempted from the scope of Regulation (EU) 2022/2554.

Art. 4.

Protection of national and commercial interests

1. This decree does not affect the responsibility of the Italian State to protect national security and its power to safeguard other essential functions of the State, including the guarantee of the territorial integrity of the State and the maintenance of public order.

2. The entities referred to in Article 3, paragraphs 6 and 7, do not include the Italian Parliament, the Judicial Authority, the Bank of Italy, and the Financial Intelligence Unit for Italy referred to in Article 6 of Legislative Decree No. 231 of 21 November 2007. The provisions of Chapter V do not apply to constitutional bodies and bodies of constitutional importance.

3. This decree does not apply to public administration bodies, organs, and branches operating in the sectors of public security, national defense, or law enforcement, including the investigation, detection, and prosecution of crimes, as well as to the security intelligence bodies referred to in Law No. 124 of August 3, 2007, and to the National Cybersecurity Agency referred to in Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021.

4. Without prejudice to the provisions of paragraph 3, one or more Prime Ministerial decrees, adopted also upon proposal of the Ministers of Justice, the Interior, and Defense, for their respective areas of competence, in agreement with the National Cybersecurity Agency, shall identify the entities that perform activities or provide services exclusively for the entities, bodies, and branches of the public administration referred to in paragraph 3, as well as in matters of civil protection. The obligations set forth in Chapter IV and the provisions of Chapter V shall not apply to these entities in carrying out such activities or services.

5. By decree of the President of the Council of Ministers, adopted pursuant to Article 43 of Law No. 124 of 3 August 2007, the entities that perform activities or provide services exclusively for the security intelligence bodies referred to in Articles 4, 6, and 7 of Law No. 124 of 2007 are identified. The obligations set forth in Chapter IV and the provisions of Chapter V do not apply to these entities in carrying out the aforementioned activities or services.

The measures adopted pursuant to the first period will be communicated to the National Cybersecurity Agency.

6. Pursuant to paragraph 4, public administration bodies, organizations, and branches with regulatory powers or whose activities are only marginally connected to the sectors referred to in the same paragraph may not be excluded. Entities acting as trust service providers may also not be excluded. The entities referred to in paragraph 4 shall ensure a level of IT security consistent with the obligations set forth in Chapter IV.

7. The obligations established in this decree do not entail the provision of information whose disclosure is contrary to the essential interests of the Italian State in matters of national security, public safety or defense.

8. Without prejudice to Article 346 of the Treaty on the Functioning of the European Union, confidential information as provided for by European Union and national legislation, in particular with regard to business confidentiality, shall be exchanged with the European Commission and the competent authorities of the Member States only to the extent necessary for the application of this Decree. The information exchanged shall be relevant and proportionate to the purpose. The exchange of information shall preserve its confidentiality and protect the security and commercial interests of essential and important entities.

Art. 5.

Jurisdiction and territoriality

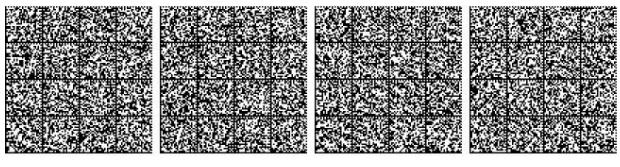
1. The entities referred to in Article 3 established on the national territory are subject to national jurisdiction, with the exception of the following cases:

(a) providers of public electronic communications networks or providers of publicly available electronic communications services, who are deemed to be under the jurisdiction of the Member State in which they provide their services; (b) providers of DNS domain name system services, top-

level domain name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content distribution network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines or social networking service platforms, who are deemed to be under the jurisdiction of the Member State in which they have their principal establishment in the Union pursuant to paragraph 2;

(c) public administration bodies, which are subject to the jurisdiction of the Member State that established them.

2. For the purposes of paragraph 1, letter *b) ,* the main establishment in the Union shall be considered to be the Member State in which decisions relating to cybersecurity risk management measures are predominantly adopted. If it is not possible to determine the Member State in which the aforementioned decisions are adopted or if they are not adopted in the Union, the main establishment shall be considered to be the one located in the Member State in which the security operations are carried out.



IT, or, where this is not possible, that of the Member State in which the interested party has the establishment with the largest number of employees in the European Union.

3. If the entities referred to in paragraph 1, letter *b)* , are they are not established in the territory of the Union but offer services within it, they shall designate a representative in the Union, who is established in one of the Member States in which the aforementioned services are offered and is subject to the relevant jurisdiction.

4. In the absence of the designation of a representative by one of the entities referred to in paragraph 3, the competent national NIS Authority may initiate legal action against the non-compliant entities.

5. The designation of the representative referred to in paragraph 3 does not prejudice any legal actions that may have already been initiated for violations of the obligations set forth in this decree, the imposition of the obligations set forth in Chapter IV and the exercise of the powers set forth in Chapter V.

Art. 6.

Essential subjects and important subjects

1. For the purposes of this decree, the following are considered essential subjects:

(a) the entities referred to in Annex I which exceed the ceilings for medium-sized enterprises referred to in Article 2, paragraph 1, of the Annex to Recommendation 2003/361/EC;

b) regardless of their size, entities identified as critical entities pursuant to the legislative decree implementing Directive (EU) 2022/2557;

(c) providers of public electronic communications networks and providers of publicly available electronic communications services referred to in Article 3, paragraph 5, letter *b)* , which are considered medium-sized enterprises pursuant to Article 2 of the Annex to Recommendation 2003/361/EC;

d) regardless of their size, qualified trust service providers and top-level domain name registries, as well as domain name system service providers referred to in Article 3, paragraph 5, letters *c)* and *d) ;*

e) regardless of their size, the central public administrations referred to in Annex III, paragraph 1, letter *a)* .

2. Without prejudice to the provisions of paragraph 1, the competent national NIS Authority shall identify, in accordance with the procedures set out in Article 40, paragraph 5, the entities referred to in Article 3, paragraphs 6, 8, 9 and 10, which, regardless of their size, are considered essential.

3. For the purposes of this decree, the subjects referred to in Article 3 which are not considered essential pursuant to paragraphs 1 and 2 of this Article are considered important subjects.

Art. 7.

Identification and listing of essential and important subjects

1. From 1 January to 28 February of each year following the date of entry into force of this decree, the entities referred to in Article 3 shall register or update their registration on the digital platform made available by the competent National Authority NIS for the purposes of carrying out the functions assigned to the National Cybersecurity Agency also pursuant to this decree. To this end, such entities shall provide or update at least the following information: *a)* the company name; *b)* the address and updated contact details, including e-mail addresses and telephone numbers; *c)* the designation of a contact point,

indicating the role within

the entity and updated contact details, including e-mail addresses and telephone numbers; *d)* where applicable,

the relevant sectors, sub-sectors and

types of subjects referred to in Annexes I, II, III and IV;

2. By March 31 of each year following the date of entry into force of this decree, the competent national NIS Authority shall draw up, in accordance with the procedures set out in Article 40, paragraph 5, the list of essential subjects and important subjects, on the basis of the registrations referred to in paragraph 1 and the decisions adopted pursuant to Articles 3, 4, and 6.

3. Through the digital platform referred to in paragraph 1, the competent national NIS Authority shall communicate to the registered entities referred to in paragraph 2: *a)*

their inclusion in the list of essential or important entities;

b) remaining on the list of essential or important subjects; *c)* being removed from

the list of subjects.

4. From 15 April to 31 May of each year following the date of entry into force of this decree, via the digital platform referred to in paragraph 1, the subjects who have received the communication referred to in paragraph 3, letters *a)* and *b)* , provide or update at least the following information:

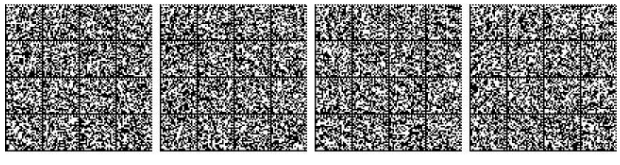
a) the public IP address space and names of the domain in use or available to the subject;

(b) where applicable, the list of Member States in which they provide services falling within the scope of this Decree;

c) the managers referred to in Article 38, paragraph 5, indicating their role within the entity and their updated contact details, including e-mail addresses and telephone numbers; *d)* a substitute for the contact

point referred to in paragraph 1, letter *c)* , indicating their role within the entity and their updated contact details, including e-mail addresses and telephone numbers.

5. Domain name system service providers, top-level domain name registries, domain name registration service providers, cloud computing service providers, data center service providers, distribution network providers



of the contents, managed service providers, managed security service providers, as well as providers of online marketplaces, providers of online search engines and providers of social network platforms, shall also provide the competent national NIS Authority, in accordance with the procedures referred to in paragraph 4:

(a) the address of the entity's head office and other establishments within the European

Union; (b) if the entity is not established within the European Union, the address of the office of its representative pursuant to Article 5, paragraph 3, together with updated contact details, including e-mail addresses and telephone numbers.

6. The competent national NIS Authority shall establish, in accordance with the procedures set out in Article 40, paragraph 5, the terms, methods and procedures for using and accessing the digital platform referred to in paragraph 1, also indicating any additional information that the subjects must provide pursuant to paragraphs 1 and 4, as well as the terms, methods and procedures for designating the representatives referred to in Article 5, paragraph 3.

7. The subjects who have received the communication referred to in paragraph 3, letters *a)* and *b) ,* shall notify the competent national NIS Authority, via the digital platform referred to in paragraph 1, of any changes to the information transmitted pursuant to this article promptly and, in any case, within fourteen days of the date of the change.

Art. 8.

Protection of personal data

1. The National Cybersecurity Agency, the NIS Sector Authorities and the entities referred to in Article 3 process personal data to the extent necessary for the purposes of this decree and in accordance with Legislative Decree 30 June 2003, n. 196 and Regulation (EU) 2016/679.

2. The processing of personal data pursuant to this Decree by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with European Union data protection legislation and European Union privacy legislation, pursuant to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.

Chapter II

NATIONAL CYBER SECURITY FRAMEWORK

Art. 9.

National Cybersecurity Strategy

1. The National Cybersecurity Strategy identifies the strategic objectives and the resources needed to achieve them, as well as appropriate strategic and regulatory measures to achieve and maintain a high level of cybersecurity.

2. The National Cybersecurity Strategy includes at least:

a) the objectives and priorities, which concern in particular to cover the sectors referred to in Annexes I, II, III and IV;

(b) a governance framework for the achievement of the objectives and priorities referred to in point *(a) ,* including the strategic measures referred to in paragraph 3;

(c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, supporting cooperation and coordination at national level between the NIS Sector Authorities, the National Cybersecurity Agency, as

National Competent Authority NIS, Single Point of Contact NIS and CSIRT Italy, as well as coordination and cooperation between these bodies and other competent authorities pursuant to sectoral legal acts of the European Union;

(d) a mechanism for identifying resources and a risk assessment at the national level; *(e)* the identification of

measures to ensure preparedness, response to, and subsequent recovery from incidents, including collaboration between the public and private sectors; *(f)* a list of the various authorities and stakeholders involved in implementing

the national cybersecurity strategy;

(g) a strategic framework for enhanced coordination between the competent authorities pursuant to this decree and the competent authorities referred to in the legislative decree transposing Directive (EU) 2022/2557 for the purposes of sharing information on both cyber and non-cyber risks, threats and incidents and of carrying out supervisory tasks, in an appropriate manner;

(h) a plan, including the necessary measures, to increase the general level of awareness of citizens regarding cyber security.

3. The following strategic measures are also envisaged within the scope of the national cybersecurity strategy: *a)* cybersecurity in the supply chain

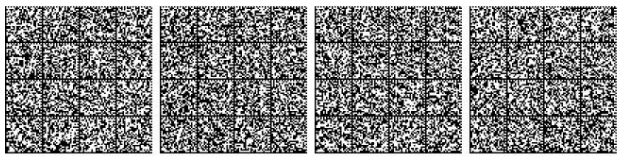
of ICT products and services used by entities to provide their services; *b)* the inclusion and definition of cybersecurity requirements for ICT products and services in public

procurement, including requirements relating to cybersecurity certification, encryption and the use of open source cybersecurity products;

(c) vulnerability management, including promoting and facilitating coordinated disclosure of vulnerabilities as referred to in Article 16; (d) supporting the general availability, integrity and

confidentiality of the public core of the open internet, including, where appropriate, cybersecurity of submarine communications cables;

(e) promoting the development and integration of relevant advanced technologies aimed at implementing cutting-edge measures in cybersecurity risk management;



(f) promoting and developing cybersecurity education, training, and awareness-raising activities, skills development, and research and development initiatives, as well as guidance on good practices and cyber hygiene controls, for citizens, stakeholders, and essential and important entities; (g) supporting academic and research institutions to develop, strengthen, and promote the deployment of cybersecurity

tools and secure network infrastructures; *(h)* developing relevant procedures and appropriate information-sharing tools to support the voluntary sharing of cybersecurity information between entities, in

compliance with European Union law; (i) strengthening benchmarks for the resilience and cyber hygiene of small and medium-sized enterprises, in particular those excluded from the scope of this Decree, by providing easily accessible guidance and support for their specific needs;

(l) promoting active cyber protection.

4. Without prejudice to the functions of the President of the Council of Ministers referred to in Article 2, paragraphs 1 and 2, of Legislative Decree no. 82 of 14 June 2021, converted, with amendments, by Law no. 109 of 4 August 2021, the National Cybersecurity Agency shall provide, pursuant to Article 7 of the aforementioned Legislative Decree no. 82 of 2021, after consulting the administrations comprising the Cybersecurity Unit, for the periodic evaluation of the National Cybersecurity Strategy, as well as its updating where necessary and in any case at least every five years on the basis of key performance indicators, proposing its adoption to the President of the Council of Ministers in accordance with the procedures set out in Article 2, paragraph 1, letter *b) ,* of the same Legislative Decree.

Art. 10.

National Competent Authority and Single Point of Contact

1. The National Cybersecurity Agency is the competent national NIS authority referred to in Article 8, paragraph 1, of Directive (EU) 2022/2555 and therefore:

a) supervises the implementation and enforcement of this decree; *b)* prepares the

measures necessary to implement this decree; *c)* carries out the regulatory functions and

activities referred to in this decree, including by adopting non-binding guidelines, recommendations and orientations;

d) identifies the essential subjects and important subjects pursuant to Articles 3 and 6, and draws up the list referred to in Article 7, paragraph 2;

e) participates in the NIS Cooperation Group, as well as in the forums and initiatives promoted at European Union level relating to the implementation of Directive (EU) 2022/2555;

f) defines the obligations referred to in Article 7, paragraph 6, and in Chapter IV; *g)* carries

out the activities and exercises the powers referred to in Chapter V.

2. The National Cybersecurity Agency shall be the NIS Single Point of Contact referred to in Article 8(3) of Directive (EU) 2022/2555, performing a liaison function to ensure cross-border cooperation of national authorities with the relevant authorities of other Member States, the Commission and ENISA.

3. For the purposes of implementing this Article, an annual expenditure of €2,000,000 is authorized starting from 2025, which is provided for pursuant to Article 44.

Art. 11.

NIS Sector Authority

1. In order to ensure the effective implementation of this decree at sector level, the NIS sector authorities are identified which support the competent national NIS authority and collaborate with it, according to the procedures set out in Article 40, paragraph 2, letter *c)* .

2. The following are designated as NIS Sector Authorities:

a) the Presidency of the Council of Ministers for:

1) the ICT services management sector, referred to in number 9 of Annex I, in collaboration with the National Cybersecurity Agency; 2) the space sector, referred

to in number 10 of Annex I; 3) the public administration sector, referred

to in Article 3, paragraphs 6 and 7; 4) in-house companies and subsidiaries or affiliates

public control, referred to in number 4 of Annex IV;

b) the Ministry of Economy and Finance, for the banking and financial market infrastructure sectors, referred to in numbers 3 and 4 of Annex I, after consulting the sector supervisory authorities, the Bank of Italy and Consob;

c) the Ministry of Business and Made in Italy for: 1) the digital

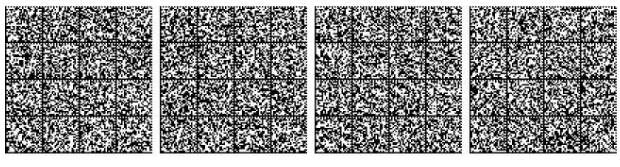
infrastructure sector, referred to in point 8 of Annex I; 2) the postal and courier services

sector, referred to in point 1 of Annex II; 3) the chemical manufacturing, production, and

distribution sector, referred to in point 3 of Annex II, after consulting the Ministry of Health;

4) the subsectors of the manufacture of computers, electronic and optical products, the manufacture of electrical equipment and the manufacture of machinery and equipment not elsewhere classified (nec), referred to respectively in letters *b) , c)* and *d)* of the manufacturing sector, referred to in number 5 of Annex II;

5) the subsectors of the manufacture of motor vehicles, trailers and semi-trailers, and the manufacture of other means of transport, referred to, respectively, in letters *e)* and *f)* of the manufacturing sector, referred to in number 5 of Annex II, after consulting the Ministry of Infrastructure and Transport;



6) digital service providers, referred to in number 6 of Annex II; *d)* the Ministry

of Agriculture, Food Sovereignty and Forestry for the food production, processing and distribution sector, referred to in number 4 of Annex II; *e)* the Ministry of the Environment and Energy Security for: 1) the energy

sector, referred to in number 1 of Annex I; 2) the drinking water supply and

distribution sector, referred to in number 6 of Annex I; 3) the

wastewater sector, referred to in number 7 of Annex I; 4) the waste management sector, referred to in number 2 of

Annex II; *f)* the Ministry of Infrastructure and Transport for: 1) the transport

sector, referred to in number 2 of Annex I; 2) entities providing transport services

local public as per number 1 of Annex IV;

g) the Ministry of University and Research for the research sector referred to in number 7 of Annex II and for the educational institutions carrying out research activities referred to in number 2 of Annex IV, also in agreement with the other supervisory administrations; *h)* the Ministry of Culture for the entities carrying

out activities of cultural interest referred to in number 3 of Annex IV; *i)* the Ministry of Health for: 1) the healthcare sector, referred to in number 5 of Annex

I; 2) the subsector of manufacturing

of medical devices and in vitro diagnostic medical devices, referred

to in letter *a)* of the manufacturing sector, referred to in number 5 of Annex II.

3. The Administrations referred to in paragraph 2, for their respective sectors and subsectors of competence, are also designated as Sector Authorities for the entities referred to in Article 3, paragraphs 9 and 10.

4. The NIS sector authorities, for their respective sectors and subsectors of competence for the purposes referred to in paragraph 1, shall proceed, in particular:

a) to verify the list of entities referred to in Article 7, paragraph 2; *b)* to support the

identification of essential and important entities pursuant to Articles 3 and 6, in particular identifying the essential and important entities referred to in paragraphs 8, 9 and 10 of Article 3; *c)* to identify the entities to which the derogations referred to in Article 3, paragraph

4 apply; *d)* to provide support for the regulatory functions and activities referred to in this decree according to the

methods referred to in Article 40; *e)* to prepare contributions for the annual report.

manual referred to in Article 12, paragraph 5, letter *c) ;*

f) to the establishment and coordination of sectoral tables, in order to contribute to the effective and coherent implementation sectoral scope of this decree and its monitoring. No attendance fees, compensation, expense reimbursements, or emoluments of any kind are provided for participation in sectoral discussions; *g)* participation in the sectoral activities of the NIS Cooperation Group

as well as in the European Union-level forums and initiatives relating to the implementation of Directive (EU) 2022/2555.

5. With an agreement signed by 30 October 2024 at the Permanent Conference for Relations between the State, the Regions and the Autonomous Provinces of Trento and Bolzano, methods of collaboration between the sector Authorities and the Regions and the Autonomous Provinces of Trento and Bolzano concerned shall be defined, when the critical entity has a regional character or operates exclusively on the territory of a Region or an Autonomous Province in the sectors referred to in paragraph 2, letters *a) ,* numbers 3 and 4, *d) , e) , f) , h)* and *i) ,* number 1.

6. In order to exercise the powers attributed by this decree, each sector authority, with the exception of that indicated in paragraph 2, letter *b) ,* is authorized to recruit, with a permanent employment contract, no. 2 units of non-managerial staff, belonging to the officials area of the current national collective agreement - Central Functions Sector, or equivalent categories, through direct transfer procedures of staff between public administrations pursuant to Article 30 of Legislative Decree no. 165 of 30 March 2001, by scrolling through existing rankings of public competitions or by initiating new public competition procedures, as well as to make use of non-managerial staff placed in command positions, pursuant to Article 17, paragraph 14, of Law no. 15 May 1997. 127, on leave of absence, secondment, or non-tenure, or any other similar arrangement provided for by the respective regulations, with the exception of teaching, educational, administrative, technical, and auxiliary staff of educational institutions. Upon non-tenure, a financially equivalent number of positions will be made unavailable within the staffing levels of the administration of origin for the entire duration of the non-tenure.

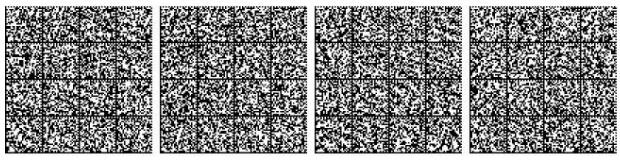
7. For the implementation of paragraph 6 of this Article, expenditure of €409,424 is authorized for the year 2024 and €925,695 annually starting from the year 2025, to be provided pursuant to Article 44.

Art. 12.

Table for the implementation of the NIS discipline

1. The NIS Implementation Committee is established on a permanent basis within the National Cybersecurity Agency to ensure the implementation and enforcement of this decree.

2. The NIS Implementation Committee is chaired by the Director General of the National Cybersecurity Agency, or his delegate, and is composed of a representative from each NIS sector authority referred to in Article 11 and two representatives designated by the regions and autonomous provinces at the Permanent Conference for Relations between the State, the Regions, and the autonomous provinces of Trento and Bolzano.



3. The members of the NIS Implementation Committee may be assisted at meetings by other representatives of their respective administrations, depending on the matters being discussed. Depending on the topics of the meetings, representatives of other administrations, universities, or research institutions and bodies, as well as private operators affected by the provisions of this decree, may also be invited to participate.

4. The NIS Implementation Committee is convened upon indication of the president or at the request of at least three members and meets at least once a quarter.

5. For the purposes referred to in paragraph 1, the NIS Implementation Table:

a) supports the competent National Authority NIS in carrying out the functions relating to the implementation and enforcement of this decree, with particular reference to the provisions of Article 10, paragraph 1, letters *a)* to *f) ; b)* formulates proposals and opinions for the adoption of initiatives,

guidelines, or policy acts for the effective implementation of this decree; *c)* prepares an annual report on the implementation of this decree.

6. Further provisions for the organization and functioning of the Roundtable may be established in accordance with the procedures set forth in Article 40, paragraph 5. No attendance fees, compensation, expense reimbursements, or other emoluments, however denominated, are provided for participation in the Roundtable for the implementation of the NIS regulations.

Art. 13.

National Cyber Crisis Management Framework

1. The National Cybersecurity Agency, acting as coordinator pursuant to Article 9, paragraph 2, of Directive (EU) 2022/2555, and the Ministry of Defence are identified as National Cyber Crisis Management Authorities, each for the areas of competence referred to in Article 2, paragraph 1, letter *g)* .

2. National IT crisis management authorities shall identify the capabilities, resources and procedures that can be used in the event of a crisis for the purposes of this decree.

3. Within twelve months of the date of entry into force of this decree, one or more decrees of the President of the Council of Ministers, upon proposal of the National Cybersecurity Agency and the Ministry of Defense, each for the areas of competence referred to in Article 2, paragraph 1, letter *g)* , after consulting the Interministerial Committee for the Security of the Republic in the composition referred to in Article 10 of Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 109 of 4 August 2021, shall define the national plan for responding to large-scale cyber incidents and crises. The plan referred to in the first sentence shall be updated periodically and, in any case, every three years.

4. The national plan for response to large-scale cyber incidents and crises establishes the objectives and the methods for managing them. This plan defines, in particular: *a)* the objectives of national

preparedness measures and activities; *b)* the tasks and responsibilities of

the national cyber crisis management authorities; *c)* cyber crisis management procedures, including their

integration into the national framework for managing crises involving cybersecurity aspects referred to in Article 10 of Legislative Decree No. 82 of 2021, and the channels for exchanging information; *d)* national preparedness measures, including exercises and training activities; *e)* the relevant public and private

sector stakeholders and the infrastructure involved; *f)* national procedures and agreements between relevant

national bodies and authorities to ensure Italy's effective support and participation in the coordinated

management of large-scale cyber incidents and crises at European Union level.

5. The decrees of the President of the Council of Ministers referred to in this article are excluded from access and are not subject to publication.

6. For the purposes of implementing paragraph 1 of this Article, an expenditure of €1,000,000 per year is authorized starting from 2025, to be provided for pursuant to Article 44.

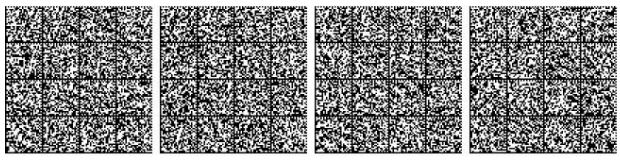
Art. 14.

Cooperation between national authorities

1. Mutual cooperation and collaboration between the competent National NIS Authority and the NIS Single Point of Contact with the central body of the Ministry of the Interior for the security and regularity of telecommunications services, referred to in Article 7 *-bis,* are ensured.
of Legislative Decree no. 144 of 27 July 2005, converted, with amendments, by Law no. 155 of 31 July 2005 (Law enforcement authorities), with the Guarantor for the protection of personal data as the supervisory authority referred to in Article 55 or 56 of Regulation (EU) 2016/679, with the National Civil Aviation Authority (ENAC) as the national authority pursuant to Regulations (EC) no. 300/2008 of the European Parliament and of the Council of 11 March 2008 and (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018, with the Agency for Digital Italy (AgID) as the supervisory body pursuant to Regulation (EU) no. 910/2014, with the Communications Regulatory Authority as the national regulatory authority pursuant to Directive (EU) 2018/1972, with the Ministry of Defence, as responsible for State defence matters, as well as with other competent national authorities also pursuant to other sectoral legal acts of the European Union, including the periodic exchange of relevant information, including with regard to significant cyber incidents and threats.

2. For the purposes of the cooperation and collaboration referred to in paragraph 1:

a) the competent national NIS Authority cooperates with the Guarantor for the protection of personal data, pursuant to



of Article 7, paragraph 5, of Legislative Decree no. 82 of 14 June 2021, converted, with amendments, by Law no. 109 of 4 August 2021, in cases of incidents involving violations of personal data, pursuant to Regulation (EU) 2016/679, without prejudice to the competence and control tasks referred to in the aforementioned regulation;

(b) where the competent national NIS authority, in the course of supervision or enforcement, becomes aware that a breach of the obligations under Article 24 by an essential or important person may lead to a personal data breach as defined in Article 4(12) of Regulation (EU) 2016/679, which must be notified pursuant to Article 33 of that Regulation, it shall inform the Italian Data Protection Authority without undue delay pursuant to Article 55 or 56 of that Regulation;

(c) where the Data Protection Authority or the supervisory authorities of other Member States referred to in Articles 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2)(i) of that Regulation, the competent National NIS Authority shall not impose administrative fines pursuant to Article 38 for an infringement referred to in point (b) of this subparagraph attributable to the same conduct. However, the competent National NIS Authority may exercise the enforcement powers referred to in Article 37;

d) by decree of the President of the Council of Ministers, upon proposal of the Minister of Defense, after consulting the National Cybersecurity Agency, the list of entities that impact the efficiency of the military instrument and the protection of the defense and military security of the State is defined, within the scope of the list referred to in Article 7, paragraph 2, on which the competent national NIS Authority shall promptly communicate to the Ministry of Defense the incidents referred to in Article 25, as well as, in the manner set out in the decree referred to in this letter, any additional cybersecurity information.

3. The cooperation and mutual collaboration of the competent National NIS Authority with the competent national authorities referred to in Regulation (EU) 2022/2554 is ensured with the tools referred to in the same Regulation (EU) 2022/2554 and in the national implementing legislation, in relation, among other things, to the periodic exchange of relevant information, including with regard to significant cyber incidents and threats.

4. The National Competent Authority for NIS shall cooperate with the relevant national competent authorities of other Member States, as referred to in Regulation (EU) 2022/2554. In particular, the National Competent Authority for NIS shall inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising its supervisory and enforcement powers to ensure compliance with the obligations under this Decree by an essential or important entity designated as a critical third-party provider of ICT services pursuant to Article 31 of Regulation (EU) 2022/2554. 5. Mutual cooperation and collaboration between the National Competent Authority for NIS and the Point of single NIS contact, in accordance with the procedures set out in Article 40, paragraph 3, with the competent national authorities and the single point of contact pursuant to Directive (EU) 2022/2557, including through the periodic exchange of information regarding the identification of critical entities, on risks, threats and incidents, both IT and non-IT, affecting the entities identified as critical pursuant to Directive (EU) 2022/2557, and on the measures taken in response to such risks, threats and incidents.

6. For the purposes of the cooperation and collaboration referred to in paragraph 5:

a) the single point of contact and the competent authorities referred to in the legislative decree transposing the directive (EU) 2022/2557 promptly communicate to the competent national authority NIS the subjects identified as critical subjects pursuant to the same legislative decree and subsequent updates;

b) the competent national authorities pursuant to the legislative decree transposing Directive (EU) 2022/2557 may request the competent national NIS Authority to carry out the activities and exercise the powers referred to in Chapter V in relation to a person who has been identified as a critical person pursuant to the aforementioned legislative decree.

Art. 15.

National Cybersecurity Incident Response Team - CSIRT Italy

1. CSIRT Italia, without prejudice to the provisions of Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 109 of 4 August 2021:

a) is the body responsible for the management functions of IT security incidents for the sectors, sub-sectors and types of entities referred to in Annexes I, II, III and IV, in accordance with the methods and procedures defined by the CSIRT itself;

(b) have an appropriate, secure and resilient information and communication infrastructure at national level through which to exchange information with essential or important actors and other relevant stakeholders; *(c)* cooperate and, where appropriate, exchange relevant information in accordance with Article 17 with sectoral or cross-sectoral communities of essential actors and important actors; *(d)* participate in the peer review referred to in Article 21;

e) ensures effective, efficient, and secure collaboration within the National CSIRT Network referred to in Article 20; *f)* pursuant to Article 7, paragraph 1, letter *s) ,* of Legislative Decree no. 82 of 2021, may establish cooperative relationships with national cybersecurity incident response teams of third countries. Within the framework of such cooperative relationships, it facilitates effective, efficient, and secure information exchange with such national CSIRTs, or equivalent national structures of third countries, using the relevant information sharing protocols, including those adopted and developed by the

the main national, European, and international communities in the sector. CSIRT Italy may exchange relevant information with National Cybersecurity Incident Response Teams of third countries or with equivalent third-country bodies, including personal data pursuant to applicable national legislation and European Union law on the protection of personal data; *g)* pursuant to Article 7, paragraph 1, letter *s)* , of Legislative Decree No. 82 of 14 June 2021, converted,

with amendments, by Law No. 109 of 4 August 2021, it may cooperate with National Cybersecurity Incident Response Teams of third countries or with equivalent third-country bodies, in particular to provide them with cybersecurity assistance.

2. The CSIRT Italy:

a) has a high level of availability of its communication channels, avoiding single points of failure, and has means that allow it to be contacted and to contact essential or important entities and other national CSIRTs at any time.

CSIRT Italy clearly indicates the communication channels and makes them known to essential and important stakeholders and other national CSIRTs; *b)* has support facilities

and information systems located in secure sites; *c)* uses an adequate system for

managing and forwarding requests, in particular to facilitate effective and efficient transfers;

d) guarantees the confidentiality and reliability of its activities; *e)* is equipped

with redundant systems and backup workspaces to ensure the continuity of its services; *f)* participates, where appropriate, in

international cooperation networks.

3. CSIRT Italy carries out the following tasks:

(a) monitors and analyzes cyber threats, vulnerabilities, and incidents at the national level and, upon request, provides assistance to essential and important stakeholders with regard to real-time or near-real-time monitoring of their information and network systems, according to a prioritization of activities defined by CSIRT Italy, in order to avoid disproportionate or excessive burdens; (b) issues early warnings, alerts, and bulletins and disseminates information to essential and important stakeholders,

as well as to competent national authorities and other relevant stakeholders, regarding cyber threats, vulnerabilities, and incidents, if possible in near-real-time;

(c) provides incident response and assistance to essential and important stakeholders, where possible; *(d)* collects and analyses forensic

data and provides dynamic risk and incident analysis as well as situational awareness regarding cyber security; *(e)* carries out, upon request of an essential or important stakeholder, in accordance with defined

modalities and procedures, a proactive scan of the information and network systems of the

interested party to detect vulnerabilities with potential significant impact; *f)* participate in the Network

of National CSIRTs referred to in Article 20 and provide mutual assistance according to its capabilities and expertise to the other members of the
Network of national CSIRTs upon their request;

(g) act as coordinator for the purposes of the coordinated vulnerability disclosure process referred to in Article 16;

h) contributes to the development of secure tools for sharing the information referred to in paragraph 1, letter *b) ; i)* may conduct, according

to defined methods and procedures, a proactive and non-intrusive scan of the publicly accessible information and network systems of essential and important entities. This scan is conducted to identify vulnerable or insecurely configured information and network systems and to inform the interested parties. This scan has no negative impact on the functioning of the entities' services.

4. CSIRT Italy applies a risk-based approach to prioritize the tasks referred to in paragraph 3.

5. In the event of malicious cybersecurity events, public structures acting as *computer emergency response teams* (CERTs) collaborate with CSIRT Italy, also for the purpose of more effective coordination of incident response.

6. CSIRT Italy establishes cooperative relationships with relevant national stakeholders in the private sector in order to pursue the objectives of this decree in relation to its own competences.

7. In order to facilitate the cooperation referred to in paragraph 5, CSIRT Italy promotes the adoption and use of standardized or common practices, classification systems, and taxonomies regarding: *a)* incident management procedures; *b)*

the coordinated disclosure of vulnerabilities pursuant

to Article 16.

8. For the purposes of implementing this Article, an annual expenditure of €2,000,000 is authorized starting from 2025, to be provided for pursuant to Article 44.

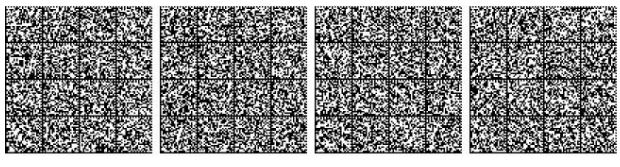
Art. 16.

Coordinated disclosure of vulnerabilities

1. CSIRT Italy is designated as coordinator for the purposes of coordinated disclosure of vulnerabilities pursuant to Article 12 of Directive (EU) 2022/2555 and acts as a trusted intermediary facilitating, if necessary, the interaction between the natural or legal person reporting the vulnerability and the manufacturer or provider of potentially vulnerable ICT services or ICT products, at the request of either party.

2. The tasks of CSIRT Italy as coordinator include:

a) the identification and contacting of the interested parties;



b) assistance to natural or legal persons who report a vulnerability;

c) the negotiation of disclosure times and the management management of vulnerabilities that affect multiple subjects.

3. Natural or legal persons may anonymously report a vulnerability to CSIRT Italy upon request. CSIRT Italy, acting as coordinator, shall ensure that diligent follow-up actions are carried out on the vulnerability report and shall guarantee the anonymity of the natural or legal person reporting it. If the reported vulnerability is likely to have a significant impact on entities in more than one Member State, CSIRT Italy shall cooperate, where appropriate, with other CSIRTs designated as coordinators within the Network of National CSIRTs referred to in Article 20.

4. The competent National NIS Authority shall adopt, in accordance with the procedures set forth in Article 40, paragraph 5, a national policy for the coordinated disclosure of vulnerabilities in line with the provisions of this decree and taking into account the non-binding guidelines of the NIS Cooperation Group. The National Cybersecurity Agency shall implement technical means to facilitate the implementation of the national policy for the coordinated disclosure of vulnerabilities.

Art. 17.

Cybersecurity Information Sharing Agreements

1. Entities falling within the scope of this Decree, and where appropriate, additional entities, may exchange, on a voluntary basis, relevant information on cyber security, including information relating to cyber threats, near-misses, vulnerabilities, techniques and procedures, indicators of compromise, adversary tactics, specific information on threat actors, cyber security alerts, and recommendations regarding the configuration of cyber security tools to detect cyber threats, if such information sharing:

(a) aims to prevent or detect incidents, recover from them, or mitigate their impact; (b) increases the level of

cybersecurity, in particular by raising awareness of cyber threats, limiting or inhibiting the ability of such threats to spread, and supporting a range of defense capabilities, vulnerability resolution and disclosure, threat detection, containment, and prevention techniques, mitigation strategies, or response and recovery phases, or by promoting collaborative research on cyber threats between public and private entities.

2. The exchange of information referred to in paragraph 1 takes place within communities of essential and important entities and, where appropriate, within their suppliers or service providers. This exchange is implemented through cybersecurity information-sharing agreements that take into account the potentially sensitive nature of the shared information.

3. The National Cybersecurity Agency, in carrying out its functions as the National Competent Authority for NIS and CSIRT Italy, shall, where possible, taking into account the non-binding guidelines and best practices developed by ENISA, facilitate the conclusion of the cybersecurity information-sharing agreements referred to in paragraph 2 and may specify the operational elements, including the use of dedicated ICT platforms and automation tools, the content, and the terms of the information-sharing agreements. When establishing the details regarding the participation of public authorities in such agreements, the National Competent Authority for NIS may impose conditions, in accordance with the procedures set out in Article 40, paragraph 5, introductory part, for the information made available by the competent authorities and CSIRT Italy. The National Cybersecurity Agency, in carrying out its functions as the competent national NIS Authority and as CSIRT Italy, supports the essential and important subjects for the application of such agreements in accordance with their strategic measures referred to in Article 9, paragraph 3, letter *h)* .

4. Essential entities and important entities shall notify the competent national NIS authority of their participation in the cybersecurity information sharing agreements referred to in paragraph 2 upon conclusion of such agreements or, where applicable, of their withdrawal from such agreements, once this has become effective.

5. Access to information regarding the list of essential and important entities is ensured for the security information bodies referred to in Articles 4, 6, and 7 of Law No. 124 of 2007, via the digital platform referred to in Article 7, the notifications referred to in Articles 25 and 26, vulnerabilities detected in the application of this decree, and any additional information beyond that referred to in this paragraph that may be deemed useful, relating to the activities referred to in this decree, subject to agreements between the aforementioned bodies and the National Cybersecurity Agency.

Chapter III

COOPERATION AT EUROPEAN UNION LEVEL AND INTERNATIONAL

Art. 18.

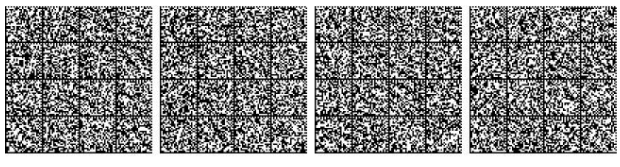
NIS Cooperation Group

1. The NIS Competent National Authority participates in the NIS Cooperation Group.

2. The NIS Sector Authorities shall participate, at the request of the competent National NIS Authority, in the initiatives of the NIS Cooperation Group relating to their sector of interest.

3. For the purposes of paragraphs 1 and 2, the competent National NIS Authority, supported by the relevant NIS Sector Authorities, shall: *a)* take into

account the non-binding guidelines of the NIS Cooperation Group on the transposition and implementation of Directive (EU) 2022/2555;



(b) take into account the non-binding guidance of the NIS Cooperation Group on the development and implementation of policies on coordinated disclosure of vulnerabilities referred to in Article 16;

(c) exchange best practices and information relating to the implementation of Directive (EU) 2022/2555, including on cyber threats, incidents, vulnerabilities, near-misses, awareness-raising initiatives, training activities, exercises and expertise, capacity building, technical specifications also adopted by a recognised standardisation body as referred to in Regulation

(EU) 1025/2012, as well as the identification of essential entities and important entities under this Decree; *d)* exchange views regarding the

implementation of sectoral legal acts of the European Union containing provisions on cybersecurity; *e)* where appropriate, discuss the reports on the reviews

between peers referred to in Article 21;

(f) request, where appropriate, a discussion on the peer review reports referred to in Article 21 involving the National Competent Authority NIS and the development of conclusions and recommendations thereon;

(g) discuss cases of mutual assistance, including the experiences and results of joint cross-border supervisory actions referred to in Article 39; (h) upon request of one or more

Member States, discuss specific requests for mutual assistance referred to in Article 39; *(i)* request, where appropriate, the discussion of specific

requests for mutual assistance referred to in Article 39 involving the National Competent Authority for NIS;

(l) exchange views on measures to mitigate the recurrence of large-scale cybersecurity incidents and crises based on lessons

learned from EU–CyCLO-Ne and the National CSIRTs Network; *(m)* participate, where necessary, in capacity-

building programmes, including through the exchange of staff between national authorities and those of other Member States; *(n)* discuss activities undertaken with regard to cybersecurity exercises, including

those carried out by ENISA; (o) participate in joint meetings with the Critical Stake Resilience Group established under Directive (EU) 2022/2557, aimed at promoting and

facilitating strategic cooperation and information exchange in the implementation of that Directive and Directive (EU) 2022/2555.

4. Furthermore, for the purposes of paragraphs 1 and 2, the competent National NIS Authority, supported by the relevant NIS Sector Authorities, shall

contribute to: *a)* the definition of non-binding guidelines for the competent authorities regarding the transposition and implementation of Directive (EU) 2022/2555;

(b) the definition of non-binding guidelines of the NIS Cooperation Group on the development and implementation of policies on coordinated disclosure of vulnerabilities referred to in Article 16;

c) the definition of non-binding opinions and cooperation with the European Commission as regards

concerns new strategic initiatives in cyber security and the coherence of sectoral IT requirements;

(d) the establishment of non-binding opinions and cooperation with the European Commission regarding draft delegated or implementing acts adopted pursuant to Directive (EU) 2022/2555; *(e)* the exchange of best practices and

information with the relevant institutions, bodies, offices and agencies of the European Union; (f) where appropriate, the preparation of conclusions and

recommendations on the peer review reports referred to in Article 21; *(g)* the preparation of coordinated risk assessments for the security of critical supply

chains in accordance with Article 22(1) of Directive (EU) 2022/2555; (h) the definition of strategic guidelines for

EU–CyCLONe and for the Network of National CSIRTs on specific emerging issues; *(i)*

strengthening cybersecurity capabilities at European Union level; (l) organising regular joint meetings

with relevant European Union private sector stakeholders to discuss the activities carried out by the

NIS Cooperation Group and gather input on emerging strategic challenges;

(m) defining the methodology and organisational aspects of the peer reviews referred to in Article 21, as well as the self-assessment methodology for Member States, and developing codes of conduct on which the working methods of the designated cybersecurity experts

referred to in that Article are based; (n) preparing reports, for the purposes of the review referred to in Article 40 of

Directive (EU) 2022/2555, on the experience gained at strategic level and from peer reviews on the implementation of that Directive;

o) to the discussion and periodic assessment of the progress of cyber threats or incidents, including ransomware;

(p) to collaborate with ENISA and the European Commission in publishing the biennial report on the state of cybersecurity in the European Union referred to in Article 18(1) of Directive (EU)

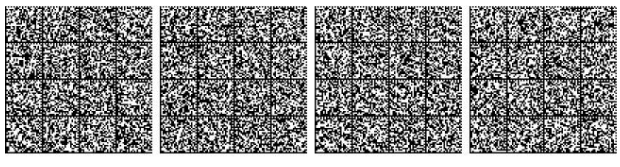
2022/2555; (q) to collaborate with ENISA, the European Commission and the Network of

National CSIRTs in defining the methodology referred to in Article 18(3) of Directive (EU) 2022/2555 for the preparation of the biennial report on the state of cybersecurity in the European Union.

Art. 19.

Network of Cyber Crisis Liaison Organizations - EU-CyCLONe

1. The National Cyber Crisis Management Authority shall participate in the Cyber Crisis Liaison Organisations Network (EU-CyCLONe).



2. For the purposes of paragraph 1, the National Cyber Crisis Management Authority contributes to:

a) increase the level of preparedness for management of large-scale computer incidents and crises;

(b) develop shared situational awareness of large-scale cyber incidents and crises; *(c)* assess the consequences and impact of large-scale

cyber incidents and crises and propose possible mitigation measures;

(d) coordinate the management of large-scale cyber incidents and crises and support decision-making at political level on such incidents and crises; *(e)* discuss, at the request of an interested

Member State, the national plans for responding to large-scale cyber incidents and crises referred to in Article 9(4) of Directive (EU) 2022/2555; (f) support collaboration with the NIS Cooperation Group in order to update it on the management of large-

scale cyber incidents and crises, as well as on trends, focusing in particular on their impact on essential and important actors; (g) cooperate with the Network of National CSIRTs; (h) prepare the report to the European Parliament and the Council on the evaluation of the work of the Network referred to in Article 16(7) of Directive (EU) 2022/2555.

3. The National Cyber Crisis Management Authority, pursuant to paragraph 2, letter *e) ,* may request to discuss the national plan for responding to large-scale cyber incidents and crises referred to in Article 13, paragraph 3.

Art. 20.

National CSIRT Network

1. CSIRT Italy participates in the National CSIRT Network.

2. For the purposes of paragraph 1, CSIRT Italy contributes to: *a)*

exchanging information regarding the ca-capacity of national CSIRTs;

(b) facilitate, where possible, the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among national CSIRTs;

(c) exchange, upon request of a national CSIRT of another Member State potentially affected by an incident, information relating to that incident, associated cyber threats, risks and vulnerabilities; *(d)* exchange information on cyber security publications and

recommendations; *(e)* ensure interoperability with regard to specifications and protocols for information exchange;

(f) upon request of a member of the National CSIRT Network potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident, its associated risks and vulnerabilities, except where

exchange of information could jeopardise the investigation of the incident; *(g)* upon

request of a member of the National CSIRTs Network, discuss and, where possible, implement a coordinated response to an incident identified in the jurisdiction of that Member State; *(h)* provide assistance to National CSIRTs of

other Member States in dealing with incidents affecting two or more Member States; *(i)* cooperate and exchange best practices with

National CSIRTs designated by other Member States as coordinators pursuant to Article 12 of the Directive

(EU) 2022/2555, as well as provide them with assistance regarding the management of coordinated disclosure of vulnerabilities that could have a significant impact on entities in more than one Member State; (l) discuss and identify further forms of operational

cooperation, including in relation to: (1) categories of cyber threats and incidents; (2) early warnings; (3)

mutual assistance; (4) principles and modalities of

coordination in

response to cross-border

risks and incidents; (5) contributions to the national plan for response to large-scale cyber incidents and

crises referred to in Article 13, paragraph 3, upon request of a Member State;

m) upon request of a member of the National CSIRT Network, discuss the capabilities and state of readiness of the requesting National CSIRT;

(n) cooperate and exchange information with regional and Union-wide cyber security operational centres in order to improve common situational awareness on cyber incidents and threats at Union level; (o) where appropriate, discuss peer review reports referred to in Article 21;

(p) exchange relevant information regarding incidents, near-misses, cyber threats, risks and vulnerabilities; (q) inform the NIS Cooperation Group about its activities and

further forms of operational cooperation discussed under point *(i)* and, if necessary, request non-binding guidance on these matters;

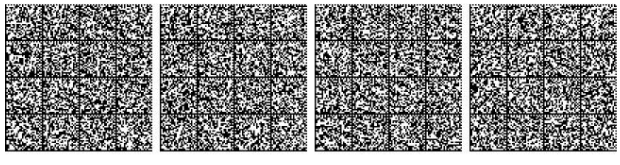
r) take stock of the results of cybersecurity exercises, including those organised by ENISA;

(s) provide non-binding guidance to facilitate convergence of operational practices in relation to the application of the provisions of this Article on operational cooperation.

Art. 21.

Peer review process

1. The National Competent Authority NIS may participate in the peer review procedure referred to in Article 19 of Directive (EU) 2022/2555, in the framework of the



methodology referred to in Article 18, paragraph 4, letter *m)* of this Decree: *a)* by requesting

the performance of a peer review in relation to the implementation of Directive (EU) 2022/2555 at the national level; *b)* by designating one or more

representatives of the National Cybersecurity Agency or the NIS Sector Authorities as cybersecurity experts, referred to in Article 19, paragraph 2, of Directive (EU) 2022/2555, to conduct peer reviews in other Member States, at their request, in compliance with the codes of conduct referred to in Article 18, paragraph 4, letter *m)* of this Decree. Any risks of conflict of interest regarding the designated cybersecurity experts shall be shared with the other Member States, the NIS Cooperation Group, the European Commission, and ENISA before the peer review begins.

2. For the purposes of paragraph 1, letter *a)* , the competent national NIS Authority, in accordance with the procedures set out in Article 40, paragraph 5,

subparagraph: *a)* shall identify at least one aspect to be submitted to peer review from among the following:

1) the level of implementation of the obligations regarding risk management measures and incident notification referred to in Articles 24 and 25; 2) the level of

capabilities, including available financial, technical and human resources, and the effectiveness of the performance of the Authority's tasks; 3) the operational capabilities of the CSIRT

Italy; 4) the status of implementation of the mutual

assistance referred to in Article 39; 5) the status of implementation of the

agreements for sharing information on cybersecurity referred to in Article 17; 6) specific issues of a cross-border or cross-sectoral nature;

(b) notify the participating Member States of the scope of the peer review, including the specific issues identified, prior to the start of the peer review; *(c)* conduct, where appropriate, a self-assessment of the aspects

covered by the review; *(d)* select suitable experts to be designated from among the IT

security experts indicated by the other participating Member States. If the competent National NIS Authority objects to the designation of one or more of the indicated experts, it shall inform the Member State stating the duly justified reasons; *(e)* provide, where appropriate, the self-assessment referred to in

letter *c)* to the designated experts referred to in letter *d) ;*

f) provides the designated experts referred to in letter *d)* the information necessary for the evaluation, including through physical or virtual on-site visits, as well as remote information exchanges; *g)* formulates, where

appropriate, observations on the report drawn up by the designated experts referred to in letter *d) ;*

h) may decide to make public the report drawn up by the designated experts referred to in letter *d) ,* to which the observations referred to in letter *g)* are attached, in whole or in part .

3. For the purposes referred to in paragraph 1, letter *b) ,* the IT security experts designated by the competent National Authority NIS: *a)* shall not disclose

to third parties any sensitive or confidential information obtained during the peer reviews in which they participate; *b)* shall participate in the activities necessary

for carrying out the peer reviews through physical or virtual on-site visits and remote information exchanges;

c) contribute to the preparation of reports on results and conclusions of peer reviews.

4. Information sharing pursuant to this Article shall be carried out in compliance with national or European Union legislation on the protection of classified information and the safeguarding of essential State functions, including national security.

Art. 22.

Communications to the European Union

1. After the date of entry into force of this decree, the Presidency of the Council of Ministers shall promptly notify the European Commission of the confirmation of the National Cybersecurity Agency as the competent National NIS Authority and as the NIS Single Point of Contact, as well as the designation of the National Cybersecurity Agency, with coordinator functions pursuant to Article 9, paragraph 2, of Directive (EU) 2022/2555, and of the Ministry of Defence, as National Cyber Crisis Management Authorities, and the related areas of competence as indicated in Article 2, paragraph 1, letter *g)* . Subsequently, any further changes to these designations or tasks shall be notified, without undue delay, to the European Commission. Appropriate forms of publicity shall be ensured for these designations.

2. The competent national NIS Authority: *a)* shall

transmit the National Cybersecurity Strategy referred to in Article 9 to the European Commission within three months of its adoption or update. Elements of the strategy relating to national security and those additional to the provisions of this decree may be excluded from the transmission;

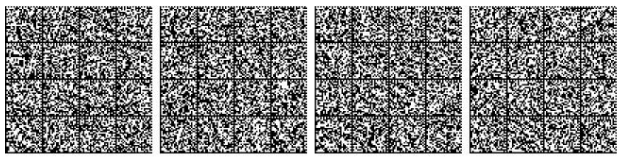
b) communicate to the European Commission by 17 January 2025 the sanctioning measures and provisions establishing sanctions against the essential and important subjects referred to in this decree.

Subsequently, any further changes to these measures and provisions shall be communicated; *c)*

communicate by 17 April 2025 and, subsequently, every two years:

1) to the European Commission and the NIS Cooperation Group, the number of essential entities and important entities included in the list referred to in Article 7, paragraph 2, for each sector and subsector referred to in Annexes I, II and III;

2) to the European Commission relevant information on the number of essential entities and important entities identified pursuant to Article 3, paragraph 9, letters *b)* to *e) ,* on the sectors and subsectors referred to in Annexes I, II and III to which they belong, on the type of service



which they provide and on the criteria referred to in Article 3, paragraph 9, letters *b)* to *e)* , for which they have been identified;

d) upon request of the European Commission, may notify it, in whole or in part, of the names of the essential and important entities referred to in letter *c)* , number 2); *e)* communicate to ENISA, without undue delay and in any case within fourteen days of receipt,

the information referred to in Article 7, paragraph 1, letters *a)* , *b)* and *d)* , paragraph 4, letter *b)* , and paragraph 5, letters *a)* and *b)* , provided by the entities referred to in the latter paragraph, for inclusion in the register referred to in Article 27 of Directive (EU) 2022/2555. The competent national NIS Authority may request access to this register from ENISA, ensuring that the confidentiality of the information contained therein is protected.

3. The NIS Single Point of Contact:

a) after the date of entry into force of this decree, communicate to the European Commission, without undue delay, the designation of the National Cybersecurity Agency as the national CSIRT, called CSIRT Italy, and as coordinator in accordance with Article 16, the respective tasks in relation to essential subjects and important subjects and any further changes thereto;

(b) submit to ENISA, every quarter starting from 1 January 2026, a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats and near-misses notified pursuant to Articles 25 and 26;

(c) transmit, after the date of entry into force of this Decree, without undue delay, the notifications of incidents with cross-border effects referred to in Articles 25 and 26 to the single points of contact of the other Member States concerned and to ENISA.

4. The National Cyber Crisis Management Authority shall communicate, within three months of the adoption or update of the national large-scale cyber incident and crisis response plan referred to in Article 13, paragraph 3, to the European Commission and the European Network of Cyber Crisis Liaison Organisations (EU-Cyclone) the relevant information relating to the requirements referred to in Article 13, paragraph 4, in relation to its national large-scale cyber incident and crisis response plan, without prejudice to Article 4, paragraphs 1, 7 and 8.

Chapter IV

RISK MANAGEMENT OBLIGATIONS FOR THE CYBER SECURITY AND INCIDENT NOTIFICATION

Art. 23.

Administrative and management bodies

1. The administrative bodies and the governing bodies of essential subjects and important subjects:

a) approve the methods of implementation of the IT security risk management measures adopted by such entities pursuant to Article 24;

b) supervise the implementation of the obligations referred to in this chapter and in Article 7;

c) are responsible for the violations referred to in this decree.

2. The administrative bodies and the governing bodies of essential subjects and important subjects:

a) are required to undergo IT security training; *b)* promote the periodic provision of training

consistent with that referred to in point *(a)* to their employees, to facilitate the acquisition of sufficient knowledge and skills to identify risks and evaluate IT security risk management practices and their impact on the entity's activities and the services offered.

3. The administrative bodies and management bodies of essential entities and important entities shall be informed on a periodic basis or, where appropriate, promptly, of the incidents and notifications referred to in Articles 25 and 26.

Art. 24.

Obligations regarding cybersecurity risk management measures

1. Essential and important entities shall adopt appropriate and proportionate technical, operational and organisational measures, in accordance with the procedures and time limits set out in Articles 30, 31 and 32, to manage the risks posed to the security of the information and network systems that such entities use in their activities or in the provision of their services, as well as to prevent or minimise the impact of incidents on the recipients of their services and on other services. Such measures shall: (a) ensure a level of security of information and network systems

appropriate to the risks involved, taking into account the most up-to-date knowledge and the state of the art in the field and, where applicable, the relevant national, European and international standards, as well as the costs of implementation; (b) be proportionate to the entity's degree of exposure to risks, its size and the likelihood of incidents

occurring, as well as their severity, including their social and economic impact.

2. The measures referred to in paragraph 1 are based on a multi-risk approach, aimed at protecting information and network systems as well as their physical environment from incidents, and include at least the following elements:

a) risk analysis and security policies information and network systems;

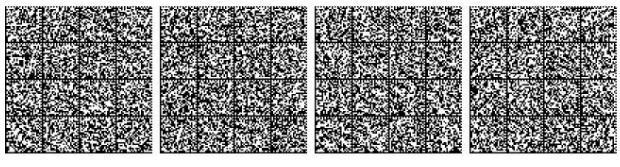
(b) incident management, including procedures and tools for making the notifications referred to in Articles 25 and 26; *(c)* business continuity,

including backup management, disaster recovery, where applicable, and crisis management; (d) supply chain security, including security aspects of the

relationship between each entity and its direct suppliers or service providers; *(e)* security of the acquisition, development and maintenance of information and network systems, including vulnerability management and

disclosure;

f) policies and procedures for evaluating the effectiveness of information security risk management measures;



g) basic hygiene practices and training in the matter cyber security ria;

h) policies and procedures relating to the use of cryptography and, where appropriate, encryption;

(i) personnel safety and reliability, access control policies, and asset and property management; *(l)* the entity's use of multi-factor

or continuous authentication solutions, secure voice, video, and text communications, and secure emergency communication systems within the entity, where appropriate.

3. In assessing which measures referred to in paragraph 2, letter *d) ,* are appropriate, entities shall take into account the specific vulnerabilities of each direct supplier and service provider and the overall quality of the products and IT security practices of their suppliers and service providers, including their secure development procedures. For the same purpose, entities shall also take into account the results of the coordinated risk assessments for the security of critical supply chains conducted by the NIS Cooperation Group.

4. Where a subject finds that it is not compliant with the measures referred to in paragraph 2, it shall, without undue delay, take all appropriate and proportionate corrective measures necessary.

Art. 25.

Accident reporting obligations

1. Essential subjects and important subjects shall notify, without undue delay, CSIRT Italia of any incident which, pursuant to paragraph 4, has a significant impact on the provision of their services, according to the methods and terms set out in Articles 30, 31 and 32.

2. The notifications include information that allows CSIRT Italy to determine any cross-border impact of the incident.

3. The notification does not expose the person making it to any greater liability than that arising from the accident.

4. An incident is considered significant if:

(a) has caused or is likely to cause serious operational disruption to services or financial losses for the data subject; (b) has had repercussions or is

likely to have repercussions on other natural or legal persons causing significant material or immaterial losses.

5. For the purposes of the notification referred to in paragraph 1, the interested parties shall transmit to CSIRT Italia:

(a) without undue delay, and in any case within 24 hours of becoming aware of the significant incident, a pre-notification which, where possible, indicates whether the significant incident can be considered the result of unlawful or malicious acts or may have a transboundary impact; (b) without undue delay, and in any case within 72 hours of

becoming aware of the significant incident, a notification of the incident which, where possible, updates the information referred to in point *(a)* and indicates an initial assessment of the significant incident, including its severity and impact, as well as, where available, indicators of compromise;

c) at the request of CSIRT Italy, an intermedia on relevant situation updates;

(d) a final report within one month of the transmission of the incident notification referred to in point *(b) ,* including: 1) a detailed description of

the incident, including its severity and impact; 2) the type of threat or the root cause (root

causes) that likely triggered the accident;

3) the mitigation measures taken and ongoing; 4) where

known, the transboundary impact of the incident;

e) in the event of an accident in progress at the time of the transsubmission of the final report referred to in point *(d) ,* monthly a progress report and a final report within one month of the conclusion of incident management.

6. By way of derogation from the provisions of paragraph 5, letter *b) ,* a trust service provider, in relation to significant incidents that have an impact on the provision of its trust services, shall provide the notification referred to in the same letter, without undue delay and in any case within 24 hours of becoming aware of the significant incident.

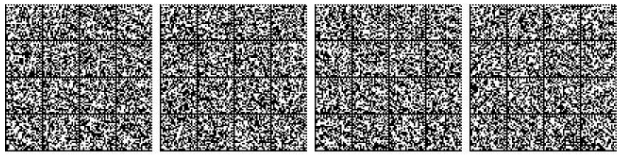
7. Without prejudice to the provisions of Article 15, paragraph 4, without undue delay and, where possible, within 24 hours of receiving the pre-notification referred to in paragraph 5, letter *a) ,* CSIRT Italy shall provide a response to the notifying entity, including initial feedback on the significant incident and, at the notifying entity's request, guidance or advice on the implementation of possible technical mitigation measures. At the notifying entity's request, CSIRT Italy shall provide additional technical support.

8. If the significant incident is suspected of being criminal in nature, CSIRT Italy also provides the notifying entity with guidance on reporting the significant incident to the central body of the Ministry of the Interior for the security and regularity of telecommunications services, pursuant to Article 7 *-bis* of Legislative Decree no. 144 of 27 July 2005, converted, with amendments, by Law no. 155 of 31 July 2005 (Law Enforcement Authority).

9. After consulting CSIRT Italia, if deemed appropriate and where possible, essential and important subjects shall communicate, without undue delay, to the recipients of their services any significant incidents that may have a negative impact on the provision of such services.

10. Essential and important entities, if deemed appropriate and where possible, after consulting CSIRT Italy, shall communicate without undue delay to the recipients of their services who are potentially affected by a significant cyber threat, corrective or mitigation measures or actions that such recipients can adopt in response to such threat. Furthermore, after consulting CSIRT Italy, if deemed appropriate, essential and important entities shall also communicate to the same recipients the nature of such significant cyber threat.

11. The National Cybersecurity Agency, in carrying out its functions as the National Competent Authority for NIS and as CSIRT Italy, also after consulting, if necessary, the competent authorities and the national CSIRTs of the other Member States concerned, may inform the public regarding



to the significant incident to prevent further significant incidents or to manage an ongoing significant incident, or if it believes that disclosure of the significant incident is otherwise in the public interest.

12. The National Cybersecurity Agency shall adopt technical means and related procedures to simplify the notifications referred to in this Article and the voluntary notifications referred to in Article 26, informing essential subjects and important subjects.

Art. 26.

Voluntary notification of relevant information

1. In addition to the incident notification obligation set out in Article 25, notifications may be sent, on a voluntary basis, to CSIRT Italy by: *a)* essential subjects and important subjects, with

regard to incidents other than those referred to in Article 25, paragraph 1, cyber threats and near-misses; *b)* subjects other than those referred to in letter *a)* , regardless of whether or not they fall within the scope of

this decree, with regard to incidents that have a significant impact on the provision of their services, cyber threats and near-misses.

2. The CSIRT Italy:

(a) handle voluntary notifications by applying the procedure referred to in Article 25;

b) handles accident notifications referred to in Article 25 prioritize voluntary notifications;

(c) process voluntary notifications only if this is the case does not constitute a disproportionate or excessive burden.

3. Without prejudice to the needs of investigation, detection and prosecution of criminal offences, the voluntary notification referred to in paragraph 1 may not have the effect of imposing on the notifying party any obligation to which he would not have been subject had he not made such notification.

Art. 27.

Use of cybersecurity certification schemes

1. In order to demonstrate compliance with certain obligations under Article 24, the competent National NIS Authority, in accordance with the procedures set out in Article 40, paragraph 5, may require essential and important entities to use categories of ICT products, ICT services and ICT processes, referred to, respectively, in Article 2, paragraph 1, letters *ff) , gg)* and *hh) ,* developed by the essential or important entity or purchased from third parties, which are certified under the European cybersecurity certification schemes referred to in Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019. The competent National NIS Authority also promotes the use of qualified trust services by essential and important entities.

2. Pending the adoption of relevant European cybersecurity certification systems referred to in Article 49 of Regulation (EU) 2019/881, the competent national NIS Authority, in accordance with the procedures set out in Article 40, paragraph 5, may require essential subjects and important subjects to use categories of pro-

ICT products, ICT services and ICT processes, developed by the essential or important entity or purchased from third parties, which are certified under certification schemes recognised at national or European level.

Art. 28.

Technical specifications

1. To promote the effective and harmonized implementation of Article 24, paragraphs 1 and 2, the competent National NIS Authority, without imposing or discriminating in favor of the use of a particular type of technology, promotes the use of European and international technical specifications, including those adopted by a recognized standardization body as per Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on the security of information and network systems.

2. For the purposes of paragraph 1, the competent National Authority for Information Security (NIS) shall take into account the non-binding guidelines and guidance developed by ENISA pursuant to Article 25(2) of Directive (EU) 2022/2555 and may draw up and periodically update a list of the categories of technologies most suitable for ensuring the effective implementation of IT security risk management measures.

3. The list referred to in paragraph 2 is not binding or exhaustive and is published on the website of the National Cybersecurity Agency in order to provide guidance on the technical specifications referred to in paragraph 1 and on the national and European sector standards applicable to the types of entities referred to in Annexes I, II, III, and IV to this decree.

Art. 29.

Domain Name Registration Database

1. In order to contribute to the security, stability and resilience of domain name systems, top-level domain name registries and domain name registration service providers shall collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence, in accordance with European Union law on the protection of personal data.

2. For the purposes of paragraph 1, the domain name registration database contains the information necessary to identify and contact the owners of the domain names and the contact points that administer the domain names present, registered or listed in the top level domain (TLD) *registry .*

Such information includes, at a minimum: *a)*

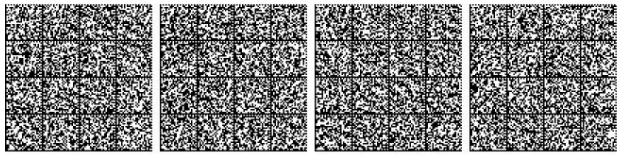
the domain name; *b)* the

registration date; *c)* the name,

contact email address and telephone number telephone number of the person carrying out the registration;

d) the contact email address and telephone number of the point of contact administering the domain name, if different from those of the person registering it.

3. Top-level domain name registries and domain name registration service providers shall establish and make public policies and



procedures, including verification procedures, to ensure that the databases referred to in paragraph 1 contain accurate and complete information.

4. Top-level domain name registries and domain name registration service providers for top-level domains shall make publicly available, without undue delay after the registration of a domain name, domain name registration data that are not personal data.

5. Top-level domain name registries and domain name registration service providers, upon reasoned request from legitimate entities, shall provide access to specific domain name registration data, in compliance with European Union data protection law. Top-level domain name registries and domain name registration service providers shall respond without undue delay and, in any case, within 72 hours of receiving the access request. This response shall contain the specific domain name registration data requested, or the reasons why the request was not deemed legitimate or duly motivated. The policies and procedures relating to the disclosure of such data shall be publicly available.

6. For the purposes of paragraph 5, the National Cybersecurity Agency may request access to domain name registration data and may enter into specific protocols with top-level domain name registries and domain name registration providers.

7. In order to avoid duplication in the collection of domain name registration data, top-level domain name registry operators and domain name registration service providers shall identify methods and procedures for collaboration in the collection and maintenance of the data referred to in paragraph 1.

Art. 30.

Listing, characterization and categorization of activities and services

1. For the purposes of Article 24, paragraph 1, from 1 May to 30 June of each year starting from the receipt of the first communication referred to in Article 7, paragraph 3, letter *a)* , the essential subjects and important subjects shall communicate and update, via the digital platform referred to in Article 7, paragraph 1, a list of their activities and services, including all the elements necessary for their characterisation and the relative attribution of a relevance category.

2. The competent national NIS Authority establishes, in accordance with the procedures set out in Article 40, paragraph 5, also taking into account the provisions of Article 25, paragraph 1, the categories of relevance as well as the process, procedures and criteria for the listing, characterisation and categorisation of the activities and services referred to in this Article.

3. Within ninety days of the communication via the digital platform referred to in paragraph 1, the competent national NIS Authority shall provide feedback to the essential and important subjects regarding the conformity of the communication with the methods and criteria referred to in paragraph 2. The aforementioned deadline may be extended by the competent national NIS Authority, for a single time and up to a maximum of an additional sixty days, If further investigation is necessary, the deadlines referred to in this paragraph shall be suspended until the aforementioned additions and information are received, which shall be provided within thirty days of the request.

4. In the absence of the response referred to in paragraph 3 from the competent national NIS Authority within the terms referred to in the same paragraph, the compliance referred to in paragraph 3 shall be deemed validated.

5. For the purposes of this Article, the competent National Authority NIS may make use of the sectoral tables referred to in Article 11, paragraph 4, letter *f)* .

Art. 31.

Proportionality and gradual nature of obligations

1. For the purposes of Articles 23, 24, 25, 27, 28 and 29, the National Competent Authority NIS shall establish proportionate obligations taking due account of the degree of exposure of entities to risks, the size of the entities and the likelihood of accidents occurring, as well as their severity, including their social and economic impact.

2. The competent national NIS Authority establishes the terms, methods, specifications and gradual implementation times of the obligations referred to in paragraph 1, according to the methods referred to in Article 40, paragraph 5, also differentiating them in relation to: *a)* the

categories of relevance referred to in Article 30, paragraph 2, of the activities and services that the information and network systems support, perform or provide;

b) the sector, subsector, and type of entity, taking into account the initial level of maturity in the field of cybersecurity; *c)* the identification of the entity as essential

or important.

3. The competent national NIS Authority shall identify, where appropriate, the circumstances that determine the suspension of the terms referred to in paragraph 2.

4. The competent national NIS authority may issue binding guidelines for the implementation of the obligations under this chapter.

5. The competent national NIS Authority may issue recommendations to support entities in implementing the obligations under this Chapter.

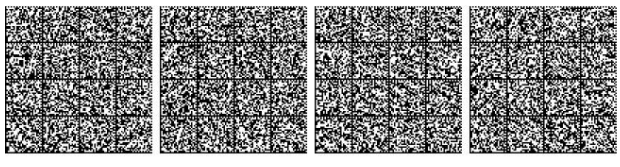
6. For the purposes of this Article, the competent National Authority NIS may make use of the sectoral tables referred to in Article 11, paragraph 4, letter *f)* .

7. Communications and interactions between the subjects and the competent national NIS Authority take place, as a priority, via the digital platform referred to in Article 7, paragraph 1.

Art. 32.

Sector-specific forecasts

1. Without prejudice to the provisions of Articles 23, 24, 25, 27, 28 and 29, taking into account the social and economic impacts of a significant incident in the supply chain of the public administration sector, the competent national authority NIS, in accordance with the procedures



The provisions referred to in Article 40, paragraph 5, may impose specific, proportionate and gradual obligations on essential and important entities that provide services, including digital ones, to the public administration.

2. The competent national NIS Authority, in accordance with the procedures set out in Article 40, paragraph 5, may identify the obligations set out in this chapter that do not apply to: *a)* the public administrations referred to in Annex III, letters *c)* and *d) ; b)* the entities referred to in Article 3, paragraph 8, paragraph 9, letter *f) ,* and paragraph 10.

3. The obligations set forth in Articles 24 and 25 do not apply to entities that exclusively provide domain name registration services. These entities shall ensure a level of IT security consistent with the obligations set forth in Articles 24 and 25.

4. The designation or failure to designate the representative referred to in Article 5, paragraph 3, does not affect the applicability of the obligations set out in this chapter.

Art. 33.

Coordination with the national cyber security perimeter discipline

1. For the purposes of Article 4:

a) the cybersecurity risk management and incident notification obligations set forth in Legislative Decree No. 105 of 21 September 2019, converted, with amendments, by Law No. 133 of 18 November 2019, are considered at least equivalent to those set forth in this decree; *b)* the provisions of this decree do not apply to the networks, information systems, and information services included in the list referred to in Article 1, paragraph 2, letter *b) ,* of Legislative Decree No. 105 of 2019. The obligations of this decree for information and network systems other than those referred to in the first sentence remain unchanged; *c)* the entities referred to in Article 1, paragraph 2 *-bis* of Legislative Decree No. 105 of 2019, are not subject to the notification obligations set forth in Article 25 of this decree for incidents , attributable to a notification made pursuant to Article 1, paragraph 3, of the same decree-law; *d)* information relating to the subjects referred to in Article 1, paragraph 2 *-bis* of Legislative Decree no. 105 of 2019, or transmitted by them to the National Cybersecurity Agency pursuant to this decree, may be exempt from the reporting obligations set forth in Article 22.

,

Chapter V

MONITORING, SUPERVISION AND ENFORCEMENT

Art. 34.

General principles for carrying out supervisory and enforcement activities

1. The competent national authority NIS monitors and evaluates compliance by essential entities and important entities with the obligations set out in Article 7 and Chapter IV, as well as the related effects on the safety of information and network systems, carrying out surveillance activities za through:

a) monitoring, analysis, and support for essential and important entities; *b)* verification and inspections; *c)* the adoption of enforcement measures; *d)* the imposition of pecuniary and additional administrative sanctions.

2. The National Competent Authority NIS may prioritise the activities referred to in this Chapter by adopting a risk-based approach.

3. The competent national NIS Authority shall ensure that the supervisory activities imposed on the subjects with regard to the obligations set forth in this decree are effective, proportionate and dissuasive, taking into account each specific case and the criteria set forth in Article 31.

4. The competent national authority (NIS) shall monitor compliance with this decree by public administration bodies, with operational independence from the public administration bodies subject to supervision.

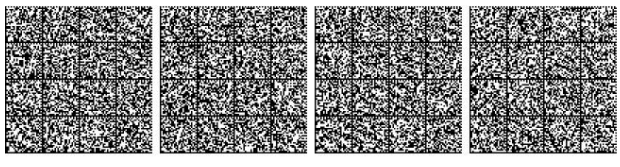
5. The competent national NIS Authority shall set out in detail the justification for adopting the measures for carrying out the activities and exercising the powers referred to in this chapter.

6. The activities and powers referred to in this chapter are respectively carried out and exercised respecting the rights of defence and taking into account the circumstances of each case and at least the following elements: *a)* the seriousness of the violation and the importance of the di-provisions violated, considering in particular serious: 1) repeated violations; 2) failure to notify or remedy significant incidents; 3) failure to remedy deficiencies following binding instructions issued by the competent National Authority NIS; 4) obstruction of the supervisory activities referred to in this Chapter; 5) provision of false or seriously inaccurate information relating to the obligations under this Decree; (b) the duration of the violation; *(c)* any relevant previous violations committed by the affected party; *(d)* any material or immaterial damage caused, including financial or economic losses, effects on other services and the number of users affected;

(e) any intentional or negligent conduct on the part of the infringer; *(f)* any measure taken by the infringer to prevent to compensate 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 national NIS Authority.

7. The periodic and targeted security audits, as well as the security scans referred to in Articles 35 and 37, shall be carried out by independent bodies and shall be based on risk assessments carried out by the national competent authority.



The NIS competent authority or the auditee, or other available information related to the risks, may request the results of such security audits and security scans, even if only partially. The costs of such security audits and security scans shall be borne by the auditee, except in duly justified cases where the NIS competent authority decides otherwise, in line with the large-scale cyber incident and crisis response plan referred to in Article 13, paragraph 3.

8. The designation or failure to designate the representative referred to in Article 5, paragraph 3, does not prejudice the performance of the activities and the exercise of the powers referred to in this chapter.

9. Communications and interactions between the subjects and the competent national NIS Authority take place, as a priority, via the digital platform referred to in Article 7, paragraph 1.

10. By decree of the President of the Council of Ministers, to be adopted in accordance with the procedures set out in Article 40, paragraph 1, the criteria, procedures and methods for carrying out the activities, exercising the powers and adopting the provisions referred to in this chapter shall be established.

Art. 35.

Monitoring, analysis and support

1. For the purposes of Article 7, the competent National Authority NIS verifies and provides feedback on the information transmitted and its compliance with the requirements prescribed for registered entities, for the purposes of inclusion in the list referred to in Article 7, paragraph 2, also ensuring adequate publicity of the criteria concerning the scope of application of this decree and the related obligations.

2. The competent national NIS Authority monitors the implementation of the obligations set forth in this decree by the entities falling within the scope of application referred to in Article 3, also implementing support interventions for these entities.

3. The competent national authority NIS, for the purposes of the at-monitoring activities referred to in paragraph 2, may:

a) request from the entities a reporting, including periodic reporting, including self-assessments and implementation plans, on the status of implementation of the obligations set forth in this decree, as well as the information necessary for the performance of their institutional tasks, declaring the purpose of the request;

(b) require entities to perform periodic or targeted security audits, particularly in the event of a significant incident or violation of this Decree by the entity concerned; (c) require entities to perform security scans based on objective,

non-discriminatory, fair, and transparent risk assessment criteria, if necessary in cooperation with the entity concerned; *(d)* issue recommendations and warnings regarding suspected violations of this Decree by the entities concerned.

4. For the purposes of paragraph 2, the competent national authority NIS shall indicate reasonable and proportionate methods and terms required to comply with, as well as to report on the status of implementation of the obligations.

5. The competent national NIS Authority analyses the results of the activities referred to in this chapter in order to establish the order of priority of the support interventions referred to in paragraph 2 and to identify the development directions of the regulation referred to in Article 31.

6. The competent national NIS authority shall implement the support measures referred to in paragraph 2 where this does not constitute a disproportionate or excessive burden.

7. The competent national NIS Authority, in carrying out the activities referred to in this chapter, may make use of the sectoral tables referred to in Article 11, paragraph 4, letter *f)* .

Art. 36.

Checks and inspections

1. The competent National Authority (NIS), in exercising its powers of verification and inspection over the entities falling within the scope of this decree, may subject the latter to: *a)* checks of the documentation and information transmitted to the competent

National Authority (NIS) pursuant to this decree; *b)* on-site and remote inspections, including random checks; *c)* requests for access to data, documents, and other

information necessary for the exercise of the powers referred to in this

article, declaring the purpose of the request and specifying the information requested from the entities.

2. With respect to important entities, the powers of verification and inspection shall apply only when the competent national NIS Authority acquires or receives evidence, indications or information suggesting possible violations of this decree.

Art. 37.

Implementing measures

1. For the purposes of exercising its enforcement powers, the competent national NIS authority shall also take into account the results of the monitoring, analysis and support activities referred to in Article 35 and the findings of the exercise of the verification and inspection powers referred to in Article 36.

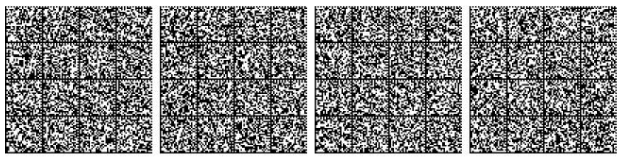
2. The competent National Authority NIS, in the exercise of its enforcement powers, may require entities, declaring the purpose, to provide data demonstrating the implementation of IT security policies, such as the results of security audits and related evidence, as well as the information necessary for the performance of its institutional tasks, including for the purposes of:

a) the assessment of IT security risk management measures; *b)* compliance with the obligations to

transmit, communicate notification and communication referred to in this decree.

3. The competent national authority NIS, in the exercise of its enforcement powers, it can order the subjects:

a) to carry out, on a periodic or targeted basis, safety audits, in particular in the event of a significant incident or violation of this decree by the entity.



The competent national NIS Authority may not require significant entities to undergo periodic security audits; (b) to carry out security scans based

on objective, non-discriminatory, fair and transparent risk assessment criteria, if necessary in cooperation with the same Authority; (c) to implement the recommendations provided following a security audit; *(d)* to

comply with the obligations set out in this Decree; *(e)* to cease and refrain from repeating

any conduct that violates this Decree; *(f)* to implement binding instructions

issued by the same Authority or to remedy any shortcomings identified in the fulfillment of the obligations set out in

this Decree or the consequences resulting from violations of this Decree; (g) for the purposes of Article 25, paragraph 9, to communicate without undue delay to the recipients of their services any significant incidents that may have a negative impact on the provision of such

services;

h) for the purposes of Article 25, paragraph 10, to communicate without undue delay to recipients of their services who are potentially affected by a significant cyber threat, any measures or corrective actions that such recipients may take in response to that threat, as well as, where appropriate, the significant cyber threat itself; *i)* for the purposes of Article 25, paragraph 11, to inform the public of incidents that have occurred; *l)*

to make public the breaches referred to in this Decree.

4. The National Cybersecurity Agency, in exercising its enforcement powers as the competent National Cybersecurity Authority, may issue binding instructions to prevent or remedy an incident.

5. The competent national NIS Authority may designate its own official to support the interested party in fulfilling the obligations set forth in this decree, with well-defined tasks over a specified period of time, including through on-site and remote visits. The interested party shall ensure full cooperation with the designated official.

6. If the interested party does not comply with the provisions set out in paragraphs 2, 3, 4 and 5, second sentence, the competent national NIS Authority shall formally warn the party to comply with such provisions.

7. For the purposes of paragraphs 2, 3, 4 and 6, the competent national NIS Authority shall indicate reasonable and proportionate methods and timeframes for complying with and reporting on the status of implementation of the obligations.

8. Before adopting the measures referred to in paragraphs 3 and 6, the competent national NIS Authority shall notify the interested parties of the preliminary conclusions, granting them a reasonable period, in any case not less than fifteen days, to submit observations.

9. Paragraph 8 does not apply where notification of preliminary findings does not permit immediate action to prevent or respond to an incident.

In such cases, the competent national NIS Authority shall justify the failure to provide the notification referred to in paragraph 8.

10. In cases where the competent national NIS Authority adopts multiple subsequent provisions relating to the same situation, paragraph 8 applies exclusively to the first of these provisions.

Art. 38.

Administrative sanctions

1. For the purposes of exercising its sanctioning powers, the competent national NIS Authority shall also take into account the results of the monitoring, support and analysis activities referred to in Article 35, the findings of the exercise of the verification and inspection powers referred to in Article 36, as well as the exercise of the enforcement powers referred to in Article 37.

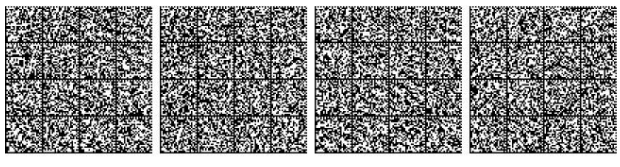
2. Without prejudice to the criteria set forth in Article 34, paragraph 6, the National Cybersecurity Agency, through one or more decisions adopted in accordance with the procedures set forth in Article 40, paragraph 5, may specify, where necessary, the criteria for determining the amount of the sanctions for the violations referred to in paragraphs 8 and 10 of this Article, adopting all necessary measures to ensure their effectiveness, proportionality, dissuasiveness, and enforcement.

3. The exercise of the powers referred to in Article 37 does not prevent the challenge of the violations referred to in paragraphs 8 and 10 of this Article, nor the related imposition of administrative sanctions referred to in this Article.

4. If the entity fails to comply within the time limits established by the formal notice referred to in Article 37, paragraphs 6 and 7, the competent National NIS Authority may temporarily suspend or request a certification or authorization body, or a judicial body, pursuant to the legislation in force, to temporarily suspend a certificate or authorization relating to part or all of the relevant services or activities performed by the essential entity. This temporary suspension shall apply until the interested party adopts the measures necessary to remedy the deficiencies or to comply with the warnings referred to in Article 37, paragraphs 6 and 7. The provisions of this paragraph shall not apply to the public administrations referred to in Annex III, nor to the entities falling within the categories referred to in Annex IV, point 1, participated in or subject to public control, and point 4, where identified according to the methods referred to in Article 40, paragraph 4.

5. Any natural person responsible for an essential entity or acting as its legal representative with the authority to represent it, make decisions on its behalf, or exercise control over it shall ensure compliance with the provisions of this decree. Such natural persons may be held liable for non-compliance in the event of a violation of this decree by the entity they represent.

6. If the subject does not comply within the terms established by the formal notice referred to in Article 37, paragraphs 6 and 7, the competent National Authority NIS may take action against the natural persons referred to in paragraph 5 of this Article, including the administrative bodies and the management bodies referred to in Article 23 of the essential subjects.



and important individuals, as well as those who perform managerial functions at the level of CEO or legal representative of an essential or important entity, the application of the additional administrative sanction of inability to perform managerial functions within the same entity. This temporary suspension is applied until the affected individual takes the necessary measures to remedy the deficiencies or comply with the warnings referred to in Article 37, paragraphs 6 and 7.

7. The provisions regarding the liability of public employees and elected or appointed officials shall apply to public employees exercising the powers referred to in paragraph 5. In particular, violation of the obligations set forth in this decree may constitute grounds for managerial, disciplinary, and administrative-accounting liability.

8. The following violations are punishable by the administrative pecuniary sanctions referred to in paragraph 9:

a) failure to comply with the obligations imposed by Article 23 on administrative bodies and management bodies, as well as with the obligations relating to IT security risk management and incident notification, pursuant to Articles 24 and 25, as regulated pursuant to Article 31;

b) failure to comply with the provisions adopted by the competent national NIS Authority pursuant to Article 37, paragraphs 3 and 4, and the related warnings.

9. The violations referred to in paragraph 8 are punishable by:

a) for essential entities, excluding public administrations, with administrative pecuniary sanctions of up to a maximum of 10,000,000 euros or 2% of the total annual worldwide turnover for the preceding financial year of the entity, calculated in accordance with the methods set out in Commission Recommendation 2003/361/EC of 6 May 2003, if this amount is higher, the minimum of which is set at one twentieth of the statutory maximum;

b) for important entities, excluding public administrations, with administrative pecuniary sanctions of up to a maximum of 7,000,000 euros or 1.4% of the total annual worldwide turnover for the preceding financial year of the entity, calculated in accordance with the methods set out in Recommendation 2003/361/EC, if this amount is higher, the minimum of which is set at one thirtieth of the statutory maximum;

c) for the public administrations referred to in Annex III, as well as for the entities included among the types referred to in Annex IV, point 1, participated in or subject to public control, and point 4, where identified according to the methods referred to in Article 40, paragraph 4, which are essential entities, with administrative pecuniary sanctions from 25,000 to 125,000 euros;

d) for the public administrations referred to in Annex III, as well as for the entities included among the types referred to in Annex IV, point 1, participated in or subject to public control, and point 4, where identified according to the methods referred to in Article 40, paragraph 4, which are important entities, the administrative pecuniary sanctions referred to in letter *c)* are reduced by one third.

10. The following violations are punishable by the administrative pecuniary sanctions referred to in paragraph 11:

a) failure to register, communicate or update information pursuant to Article 7, paragraphs 1, 3, 4, 5 and 7; *b)* failure to comply with the procedures

established by the Authority
competent national NIS pursuant to Article 7;

c) failure to communicate or update the list of activities and services as well as their categorization pursuant to Article 30,

paragraph 1;

d) failure to implement or enforce the obligations relating to the use of certification schemes, the domain name registration database and the specific sectoral provisions referred to in Articles 27, 29 and 32, as regulated pursuant to Article 31. *e)* failure to collaborate with the competent national NIS Authority in carrying

out the activities and exercising the powers referred to in this chapter;

f) failure to collaborate with CSIRT Italy.

11. The violations referred to in paragraph 10, without prejudice to the

The following are punishable by the minimum edicts referred to in paragraph 9:

a) for essential entities, with administrative pecuniary sanctions of up to a maximum of 0.1% of the total annual worldwide turnover for the preceding financial year of the entity, calculated in accordance with the methods set out in Recommendation 2003/361/EC; *b)* for important entities, with administrative pecuniary

sanctions of up to a maximum of 0.07% of the total annual worldwide turnover for the preceding financial year of the entity, calculated in accordance with the methods set out in Recommendation 2003/361/EC;

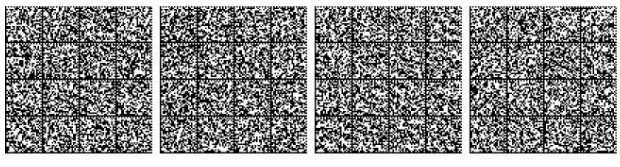
c) for the public administrations referred to in Annex III, as well as for the entities included among the types referred to in Annex IV, point 1, participated in or subject to public control, and point 4, where identified according to the methods referred to in Article 40, paragraph 4, which are essential entities, with administrative pecuniary sanctions from €10,000 to €50,000; *d)* for the public administrations referred to in Annex III, as well as for the entities

included among the types referred to in Annex IV, point 1, participated in or subject to public control, and point 4, where identified according to the methods referred to in Article 40, paragraph 4, which are important entities, the administrative pecuniary sanctions referred to in letter *c)* are reduced by one third.

12. The violations referred to in this article are repeated in the cases governed by Article 8 -*bis* of Law No. 689 of November 24, 1981. In cases of specific repetition, the penalty provided for the violation is increased up to double. In cases of non-specific repetition, the penalty provided for the most serious violation is applied, increased up to three times.

13. In the event of failure to register or late registration as per Article 7, all violations set out in paragraphs 8 and 10 of this Article shall be contested in any case, and the sanction set out for the most serious violation shall be applied, increased up to three times.

14. In the event of failure to comply with the obligations relating to the notification of incidents pursuant to Article 25, by the public administrations referred to in Annex III, as well as by the entities falling within the categories referred to in Annex IV, point 1, participated in or subjected to public control



blico, and point 4, where identified according to the methods set out in Article 40, paragraph 4, the provisions set out in paragraph 9 of this Article shall apply only in the event of a specific repetition within a period of five years and the competent National Authority NIS may exercise, during the twelve months following the ascertainment of the violation, the verification and inspection powers set out in Article 36.

15. For the purposes of implementing this article, the methods of application of the following litigation-deflationary tools within the scope of the sanctioning procedure are identified pursuant to Article 40, paragraph 1, letter *c) :*

a) the invitation to comply that the competent national NIS Authority, if it ascertains the existence of violations, and except in the case of repeated violations, sends to the violator, assigning a suitable peremptory deadline, proportionate to the type and severity of the violation, to conform the conduct to the obligations set forth in the applicable legislation. If the violator complies with the obligation to conform the conduct within the established timeframe, the sanctioning procedure does not continue. The provision set forth in this letter does not apply to the person who has already been the recipient of the warning referred to in Article 37, paragraph 6, or to the persons and in the cases set forth in paragraph 14 of this Article; *b)* the option to terminate the proceedings by paying a reduced amount equal to one-third of the maximum fine

or, if more favorable, double the minimum fine, if established, within a mandatory period of sixty days from the date of notification of the dispute. In the event of reiteration, Article 8 -*bis* of Law No. 689 of November 24, 1981, applies;

c) cases in which the imposition of administrative sanctions is not subject to publicity.

16. The proceeds of the administrative pecuniary sanctions imposed by the competent National Authority (NIS) pursuant to the provisions of this decree shall be paid into the State budget to be reallocated to the appropriate chapter of the expenditure estimates of the Ministry of Economy and Finance, pursuant to Article 18 of Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021, to increase the budget of the National Cybersecurity Agency.

Art. 39.

Mutual assistance

1. The competent national NIS authority shall cooperate with and assist the competent authorities of the other Member States concerned, and may request their cooperation and mutual assistance, as necessary, in the following cases:

(a) an entity considered to be under national jurisdiction pursuant to Article 5 or whose information and network systems are located on the national territory, provides services in one or more other Member States; (b) an entity

considered to be under the jurisdiction of other Member States pursuant to Article 5 or whose information and network systems are located on the territory of other Member States, provides services on the national territory.

2. The cooperation referred to in paragraph 1 includes mutual: *a)* notification

and consultation, through the NIS Single Point of Contact, regarding inspection activities, enforcement measures, and the exercise of sanctioning powers, as well as their application; *b)* justified requests for inspection

activities or the adoption of enforcement measures; *c)* assistance proportionate to the

respective resources so that inspection and enforcement activities can be implemented effectively, efficiently, and consistently.

3. The mutual assistance referred to in paragraph 2, letter *c) ,* may concern requests for information and inspection activities, including requests to carry out *on-site* or remote inspections or targeted safety audits.

4. The competent national NIS authority may reject a request for assistance from competent authorities of other Member States pursuant to this Article when: *a)* the competent national NIS authority is not

competent to provide the requested assistance; *b)* the requested assistance is not proportionate to the inspection

and enforcement tasks provided for in this decree; *c)* the request concerns information or involves activities which, if disclosed

or carried out, would be contrary to the essential interests of national security, public security or defence of the State.

5. For the purposes of paragraph 4, before rejecting a request, the competent national NIS authority shall consult the competent authorities of the Member States concerned. At the request of one of the Member States concerned, the competent national NIS authority shall also consult the European Commission and ENISA.

6. Where appropriate and by mutual agreement, the National Competent Authority NIS and the competent authorities of other Member States may carry out joint inspection and enforcement activities.

7. The competent national NIS authority may:

(a) upon a request for mutual assistance from competent authorities of other Member States, exercise the powers referred to in this Chapter towards a person who meets the criteria set out in paragraph 1, letter *a)* of this Article; (b) forward a request for mutual assistance to the competent

authorities of the other Member States concerned for the exercise of their respective powers referred to in Chapter VII of Directive 2022/2555 towards a person who meets the criteria set out in paragraph 1, letter *b)* of this Article.

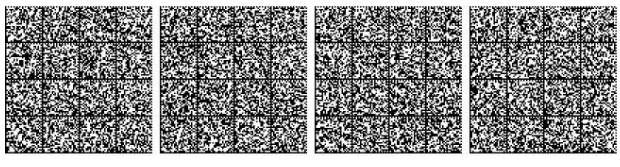
Chapter VI

FINAL AND TRANSITIONAL PROVISIONS

Art. 40.

Implementation

1. With one or more decrees of the President of the Council of Ministers, adopted also in derogation from Article 17 of Law No. 400 of 23 August 1988, upon proposal of the National Cybersecurity Agency, after consulting the Table for the at-



implementation of the NIS regulation referred to in Article 12 and following the opinion of the Interministerial Committee for Cybersecurity, referred to in Article 4 of Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 109 of 4 August 2021: *a)* the criteria for the application

of the clause are defined
safeguard only as per Article 3, paragraph 4;

b) the criteria, procedures, and methods referred to in Article 34, paragraph 10, are established; *c)* the

methods of applying, within the scope of the sanctioning procedure, the dispute-deflation tools referred to in Article 38, paragraph 15, are identified.

2. By means of one or more decrees of the President of the Council of Ministers, adopted also in derogation from Article 17 of Law No. 400 of 23 August 1988, upon proposal of the National Cybersecurity Agency, in agreement with the relevant NIS sector authorities, after consulting the NIS Regulation Implementation Committee and following the opinion of the Interministerial Committee for Cybersecurity: *a)* additional criteria may be established for identifying the

types of entities referred to in Annexes I and II, as well as the additional types of entities referred to in Article 3;

b) further categories of public administrations referred to in Article 3, paragraphs 6 and 7, to which this decree applies may be identified;

c) the methods of coordination and collaboration between the National Cybersecurity Agency and the NIS sector authorities are established for the purposes of this decree.

3. One or more Prime Ministerial Decrees, adopted in derogation from Article 17 of Law No. 400 of 23 August 1988, upon proposal of the National Cybersecurity Agency, in agreement with the relevant Administrations, after consulting the Committee for the Implementation of the NIS Regulations, and after consulting the Interministerial Committee for Cybersecurity, shall establish, where necessary, the coordination and collaboration methods referred to in Article 14.

4. With one or more decisions of the National Cybersecurity Agency, upon proposal of the relevant NIS sector Authorities, after consulting the Table for the implementation of the NIS discipline: *a)* the subjects to whom the safeguard

clause referred to in Article 3, paragraph 4, applies are identified, where necessary;

b) the subjects to whom the regulation applies are identified this decree pursuant to Article 3, paragraphs 8 and 9.

5. With one or more decisions of the National Cybersecurity Agency, after consulting the Committee for the Implementation of the NIS Regulation: *a)* pursuant to

Articles 3 and 6, the list of essential and important subjects referred to in Article 7, paragraph 2 is established; *b)* the terms, methods and procedures

for use and access referred to in Article 7, paragraph 6, any additional information that the subjects must provide pursuant to paragraphs 1 and 4 of the same article are established, as well as the terms, methods and procedures for designating the representatives referred to in Article 5, paragraph 3;

c) further provisions may be defined for the organization and functioning of the Table for the implementation of the NIS discipline referred to in Article 12;

d) the national policy for the coordinated disclosure of vulnerabilities referred to in Article 16, paragraph 4 is adopted, in agreement with the Ministry of Justice; *e)* conditions

may be imposed on the information made available by the competent authorities and by CSIRT Italy in the context of the information sharing agreements on cybersecurity referred to in Article 17, paragraph 3; *f)* the methods by which essential subjects and important subjects notify the

competent national NIS Authority of their participation in the information sharing agreements on cybersecurity referred to in Article 17, paragraph 4 are established;

g) the IT security experts referred to in Article 21, paragraph 1, may be designated, and, if necessary, the methods for carrying out the peer review referred to in the same Article 21 may be identified;

h) the use of certified ICT products, ICT services and ICT processes referred to in Article 27 may be imposed, defining the related terms, criteria and methods;

(i) the categories of relevance as well as the methods and criteria for the listing, characterisation and categorisation of the activities and services, of multi-sectoral and, where appropriate, sectoral value, referred to in Article 30 are established;

l) proportionate and gradual obligations are established, with multi-sectoral and, where appropriate, sectoral scope, as per Article 31, the methods of applying the same obligations for entities carrying out activities in multiple sectors or sub-sectors and for the entities referred to in Article 32, paragraphs 1 and 2; *m)* the criteria for determining the amount of sanctions pursuant to Article 38, paragraph 2 are established.

6. The following are excluded from access and are not subject to publication: *a)* the

decrees referred to in paragraph 3;

b) the decisions referred to in paragraph 4, letter *b)* , and paragraph 5, letter *a)* ; *c)*

records, documents, and information relating to or in any way connected to incident notifications or whose disclosure or access could in any case cause possible harm to national security in cyberspace.

7. Within thirty days of the date of entry into force of this decree, the following shall be adopted: *a)* the

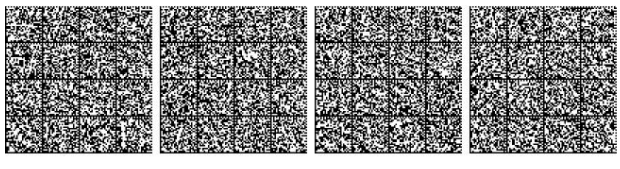
decrees of the President of the Council of Ministers referred to in paragraph 1, letter *a)* , and paragraph 3; *b)* the

decisions of the National Cybersecurity Agency referred to in paragraph 4, letter *b)* , and paragraph 5, letters *b)* and *c)* .

8. Within six months of the date of entry into force of this decree, the following shall be adopted:

a) the decrees of the President of the Council of Ministers referred to in paragraph 1, letters *b)* and *c)* , and in paragraph 2, letter *c)* ; *b)*

the decisions of the Agency for Cybersecurity national security referred to in paragraph 5, letters *d)* , *f)* and *l)* .



9. Within eighteen months of the date of entry into force of this decree, the decisions of the National Cybersecurity Agency referred to in paragraph 5, letter *i)* shall be adopted .

10. The decrees of the President of the Council of Ministers referred to in this article are updated periodically and, in any case, every three years.

11. The decisions of the National Cybersecurity Agency referred to in this article are updated periodically and, in any case, every two years.

Art. 41.

Transitional regime and repeals

1. The provisions of this decree shall apply from 18 October 2024.

2. Starting from 18 October 2024, Legislative Decree no. 65 of 18 May 2018 is repealed, with the exception of Article 7, paragraph 8, and Article 8, paragraph 10, which are repealed from 1 January 2025. Chapters IV and V of the same Legislative Decree no. 65 of 2018 continue to apply only to the subjects referred to in Article 3, paragraph 9, letter *a) ,* until the date of adoption of the implementing provisions referred to in Article 40, paragraphs 1, 2, 3, 4 and 5, letters *a) , b) , e)* and *f) .*

3. The following amendments are made to the Electronic Communications Code, pursuant to Legislative Decree No. 259 of 1 August 2003: *a)* Article 2,

paragraph 1, letter *h)* is repealed; *b)* Article 30, paragraph 26,

and Articles 40 and 41 are repealed.

4. The implementing provisions of Articles 40 and 41 of the Code referred to in Legislative Decree no. 259 of 2003 shall continue to apply, to the extent not in conflict with the law and the provisions of this decree, until the adoption of the decisions referred to in Article 40, paragraph 5, letter *l) .*

Art. 42.

First application phase

1. During the initial application phase:

a) pursuant to Article 7, by January 17, 2025, domain name system service providers, top-level domain name registries, domain name registration service providers, cloud computing service providers, data center service providers, content distribution network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines, and social network service platforms falling within the scope of this decree, shall register on the digital platform referred to in Article 7, paragraph 1; *b)* until December 31, 2025, the Table for the Implementation of the NIS Regulation referred to in Article 12 shall meet at least once every sixty days; *c)* until 31 December 2025, the deadline for fulfilling the obligations

referred to in Article 25 is set at nine months from receipt of the communication referred to in Article 7, paragraph 3, letters *a)* and *b) ,* and the deadline for fulfilling the obligations

referred to in Articles 23, 24 and 29 is set at eighteen months from the same communication.

tion. For the purposes referred to in the first paragraph, the competent national NIS Authority may establish basic methods and specifications to ensure compliance by essential and important entities.

2. The obligation referred to in Article 30, paragraph 1, applies from 1 January 2026.

3. Pursuant to Article 7, paragraph 1, essential subjects and important subjects may register starting from the date of publication of the platform referred to in the same paragraph.

Art. 43.

Regulatory changes

1. In order to ensure consistency with the national cybersecurity architecture and the tasks of the National Cybersecurity Agency, the following amendments are made to Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021:

a) in Article 1, paragraph 1: 1)

letter *d)* is replaced by the following:

« d) NIS Legislative Decree, the legislative decree transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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;»; 2) in letter *e) ,* the words: «referred to in Article 6» are replaced by the following: «referred to

in Article 9»; *b)* in Article 7: 1) in paragraph 1: 1.1) letter *d)* is replaced by the following:

« d) is the competent national NIS Authority and Single NIS contact point referred to in Article 2, paragraph 1, letters *d)* and *e) ,* of the NIS legislative decree, to protect the legal unity of the system;

d *-bis)* is the National Authority for the Management of Information Technology Crises referred to in Article 2, paragraph 1, letter *g) ,* of the NIS Legislative

Decree; d *-ter)* is the national CSIRT, called CSIRT Italia, referred to in Article 2, paragraph 1, letter *i) ,* of the NIS Legislative Decree;»; 1.2) in

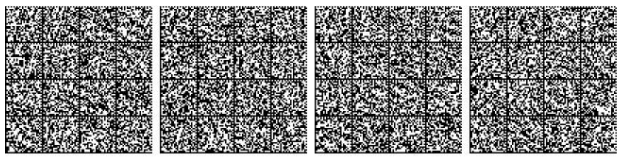
letter *n) ,* the words: «CSIRT Italia referred to in Article 8» are replaced by the following «CSIRT Italia referred to in Article 2, paragraph 1, letter *i) »;*

1.3) in letter n *-bis),* the words: «referred to in article 3, paragraph 1, letters *g)* and *i) »* are replaced by the following: «the essential subjects and important subjects referred to in article 6 of the NIS legislative decree»; 2) paragraph 3 is repealed;

c) Article 15 is repealed.

2. To ensure consistency with the obligations set out in Chapter IV and with the provisions set out in Chapter V of this decree, the following amendments are made to Article 1 of Legislative Decree No. 105 of 21 September 2019, converted, with amendments, by Law No. 133 of 18 November 2019:

a) paragraph 3 *-bis* is repealed;



b) paragraph 8 is replaced by the following: "8.

The incident notification pursuant to paragraph 3, letter *a)* , carried out by the entities included in the national cyber security perimeter that fall within the scope of the legislative decree transposing Directive (EU) 2022/2555 fulfills the obligations regarding incident notification pursuant to Article 25 of the same legislative decree."; *c)* after paragraph 8, the following is inserted: The obligations set out in Chapter IV and the inspection

and sanctioning activities set out in Chapter V

«8 -*bis*. provided for essential entities pursuant to the same legislative decree shall apply to entities included in the national cybersecurity perimeter that are not identified as essential or important entities pursuant to Articles 3 and 6 of the Legislative Decree transposing Directive (EU) 2022/2555, limited to information and network systems other than those included in the list of networks, information systems and IT services referred to in Article 1, paragraph 2, letter *b)* , of this decree. The National Cybersecurity Agency, after consulting the interministerial committee for the implementation of the national cybersecurity perimeter, shall establish with its own resolution the terms, methods, specifications and gradual implementation times of the obligations set out in this paragraph."; *d)* paragraph 17 is repealed.

Art. 44.

Financial provisions

1. ICT expenses incurred by public administrations pursuant to Articles 10, 11, 13, and 15 of this decree and, more generally, ICT expenses incurred to adapt information systems to this decree, are consistent with the Three-Year Plan for Information Technology in Public Administration pursuant to Article 1, paragraphs 512 to 520, of Law No. 208 of 28 December 2015.

2. The costs arising from Articles 10, paragraph 3, 11, paragraph 7, 13, paragraph 6, and 15, paragraph 8, equal to 409,424 euros for the year 2024 and 5,925,695 euros per year starting from the year 2025, are provided for:

a) €409,424 for the year 2024, €2,625,695 for the year 2025, €2,707,695 for the year 2026 and €3,100,695 per year starting from the year 2027, through a corresponding reduction in the Fund for the implementation of the European legislation referred to in Article 41 -*bis* of Law No. 234 of 24 December 2012; *b)*

€3,300,000 for the year 2025, €3,218,000 for the year 2026, and €2,825,000 annually starting from the year 2027, through the use of resources resulting from the repeal referred to in paragraph 2 of Article 41.

3. Except as provided in paragraph 2, the implementation of this decree must not result in new or increased burdens on public finances. The competent administrations shall provide for this within the human, instrumental, and financial resources available under current legislation.

This decree, bearing the State seal, will be included in the Official Collection of the normative acts of the Italian Republic. Anyone who is entitled to it is obliged to observe it and have it observed.

Given in Rome, this 4th day of September 2024

MATTARELLA

MELONI, *President of the Council of Ministers*

FITTO, *Minister for European Affairs, the South, Cohesion Policies and the PNRR*

ZANGRILLO, *Minister for Public Administration*
no

TAJANI, *Minister of Foreign Affairs and International Cooperation*

PIANTEDOSI, *Minister of the Interior*

NORDIO, *Minister of Justice*

CROSETTO, *Minister of Defense*

GIORGETTI, *Minister of Economy and Finance*

URSO, *Minister of Enterprise and Made in Italy*

LOLLOBRIGIDA, *Minister agriculture, food sovereignty and forests*

PICHETTO FRATEN, *Minister of the Environment and Safety*
energy security

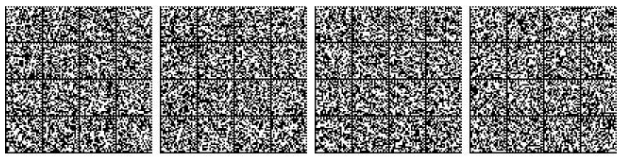
SALVINI, *Minister of Infrastructure and Transport*

BERNINI, *Minister of Universities and Research*

SANGIULIANO, *Minister of Culture*

SCHILLACI, *Minister of Health*

Seen, *the Keeper of the Seals:* NORDIO



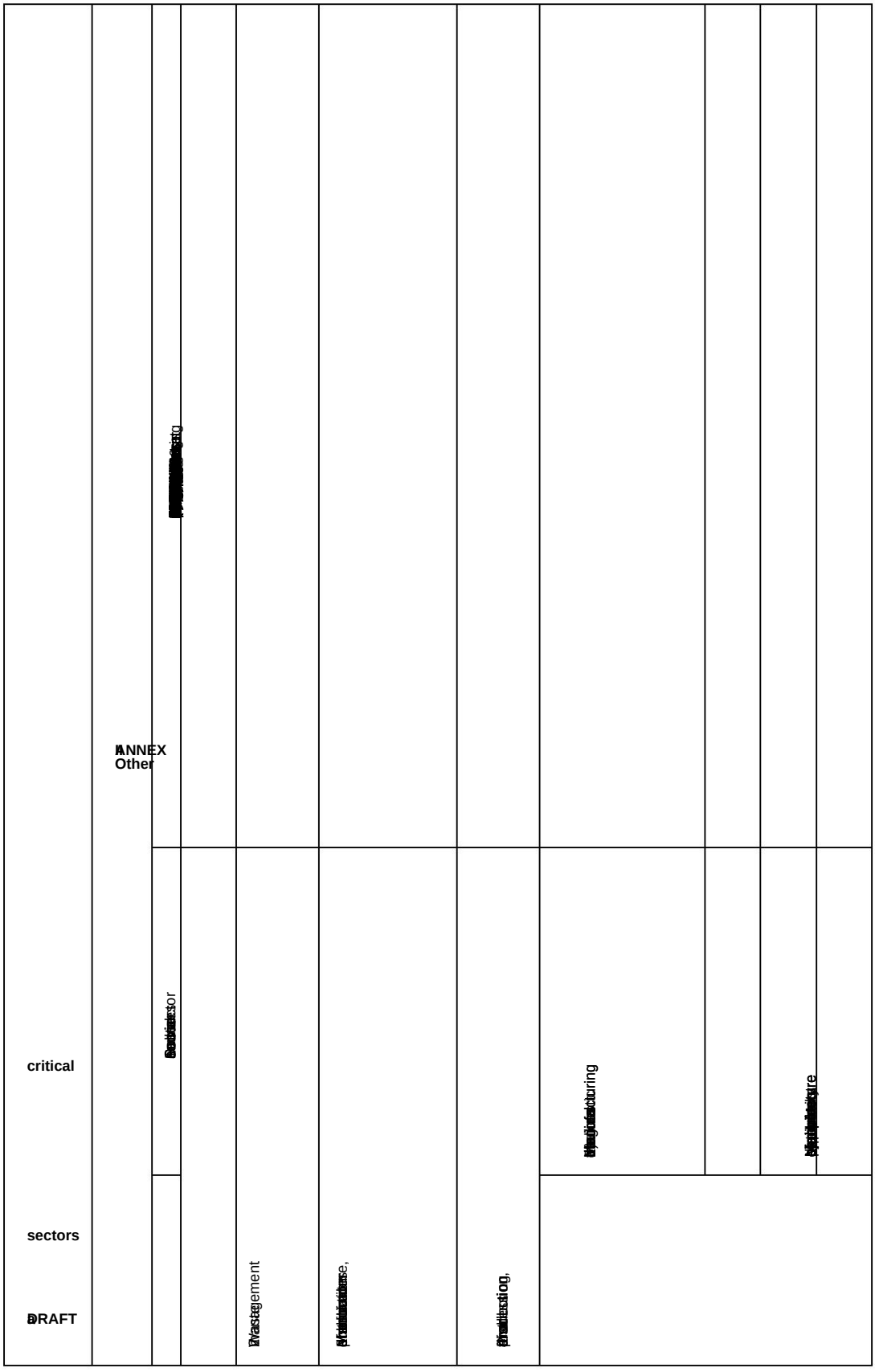
ANNEX

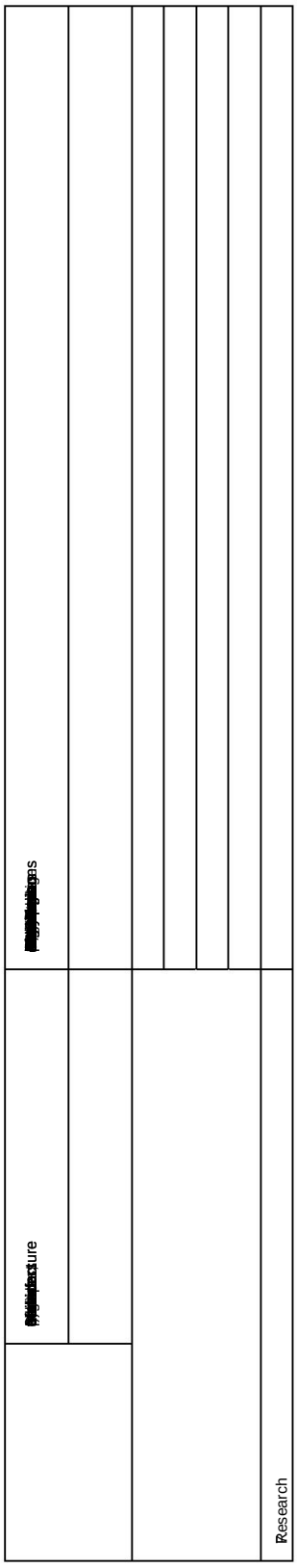
Sectors with high criticality

Sector	Subsector	Subject type
		[illegible]
	[illegible]	
		[illegible]
	Gas	

		[illegible]
Banking Sector		
Financial market infrastructure		
Health sector		
Drinking water		
Wastewater		
Digital infrastructures		

Domain *system*	
Type	
[illegible]	
Providers	
—	
Providers	
[illegible] applications	
[illegible] applications	
Providers	[illegible]
[illegible]	
[illegible] applications	[illegible] management





DRAFT LEGISLATIVE DECREE IMPLEMENTING NIS2

Implementation of Directive (EU) 2022/2555 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

ANNEX III Central,

regional, local and other administrations 1. For the purposes of Article 3, paragraph 6, the following categories are identified:

a) central administrations:
1) the constitutional bodies and those of constitutional importance; 2) the Presidency of the Council of Ministers and the Ministries; 3) the tax agencies; 4) the independent administrative authorities;

b) regional administrations: 1. the Regions and autonomous Provinces.

c) local administrations
1. Metropolitan cities; 2. Municipalities with a population greater than 100,000; 3. Regional capitals; 4. Local health authorities.

d) other public entities:
1. Bodies regulating economic activity; 2. Bodies producing economic services; 3. Bodies with an associative structure; 4. Bodies producing welfare, recreational, and cultural services; 5. Research bodies and institutions; 6. Experimental zooprophylactic institutes.

DRAFT LEGISLATIVE DECREE IMPLEMENTING NIS2

Implementation of Directive (EU) 2022/2555 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

ANNEX IV

Further types of subjects

1. Entities providing local public transport services.
2. Educational institutions carrying out research activities.
3. Entities carrying out activities of cultural interest.
4. *In* -house companies, subsidiary companies and publicly controlled companies, as defined in Legislative Decree 19 August 2016, n. 175.

NOTE

WARNING:

The text of the notes published here was drafted by the competent administration, pursuant to Article 10, paragraphs 2 and 3, of the Consolidated Law on the Promulgation of Laws, the Issuance of Presidential Decrees, and the Official Publications of the Italian Republic, approved by Presidential Decree No. 1092 of December 28, 1985, for the sole purpose of facilitating the reading of the provisions of the law, whether amended or to which reference is made. The validity and effectiveness of the legislative acts transcribed here remain unchanged.

For EEC directives, the publication details in the *Official Journal* of the European Communities (OJEU) are provided.

Notes to the preamble:

Article 76 of the Constitution establishes that the exercise of the legislative function cannot be delegated to the Government unless principles and guidelines are established and only for a limited time and for specific purposes.

Article 87, fifth paragraph, of the Constitution grants the President of the Republic the power to promulgate laws and issue decrees. having the force of law and regulations.

— Article 14 of Law No. 400 of August 23, 1988 (Regulation of Government Activity and Organization of the Presidency of the Council of Ministers), published in the *Official Journal* No. 214 of September 12, 1988, SO, is reported below:

«Art. 14 *(Legislative decrees)* . — 1. Legislative decrees adopted by the Government pursuant to Article 76 of the Constitution are issued by the President of the Republic with the name of "legislative decree" and with an indication, in the preamble, of the delegating law, the resolution of the Council of Ministers, and the other procedural requirements prescribed by the delegating law.

2. The legislative decree must be issued within the deadline set by the delegation law; the text of the legislative decree adopted by the Government is transmitted to the President of the Republic, for issuance, at least twenty days before the deadline.

3. If the legislative delegation refers to a number of distinct matters subject to separate regulation, the Government may exercise it through several successive acts for one or more of the aforementioned matters. In relation to the final deadline established by the delegation law, the Government periodically informs the Chambers of the criteria it follows in organizing the exercise of the delegation.

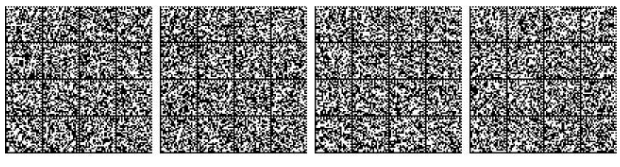
4. In any case, if the deadline for exercising the delegation exceeds two years, the Government is required to request the opinion of the Chambers on the draft delegated decrees. The opinion is expressed by the Standing Committees of the two Chambers competent for the subject matter within sixty days, specifically indicating any provisions deemed not to correspond to the directives of the delegation law. The Government, within the following thirty days, having examined the opinion, retransmits the texts, with its observations and any amendments, to the Committees for a final opinion, which must be expressed within thirty days.

— Articles 31 and 32 of Law No. 234 of 24 December 2012 (General provisions on Italy's participation in the training and for the implementation of European Union legislation and policies), published in the *Official Journal of* 4 January 2013, no. 3:

«Art. 31 *(Procedures for the exercise of legislative delegations conferred on the Government by the European delegation law)* . — 1. In relation to the legislative delegations granted by the European delegation law for the transposition of the directives, the Government shall adopt the legislative decrees within the four-month deadline prior to the transposition deadline indicated in each of the directives; for the directives whose deadline thus determined has already expired on the date of entry into force of the European delegation law, or expires within the following three months, the Government shall adopt the transposition legislative decrees within three months of the date of entry into force of the same law; for the directives that do not provide for a transposition deadline, the Government shall adopt the relevant legislative decrees within twelve months of the date of entry into force of the European delegation law.

2. Legislative decrees are adopted, in compliance with Article 14 of Law No. 400 of 23 August 1988, upon proposal of the President of the Council of Ministers or the Minister for European Affairs and the Minister with primary jurisdiction over the matter, in consultation with the Ministers of Foreign Affairs, Justice, Economy and Finance, and other Ministers interested in the subject matter of the directive. Legislative decrees are accompanied by a correlation table between their provisions and those of the directive to be transposed, prepared by the administration with primary institutional jurisdiction over the matter.

3. The European delegation law indicates the directives for which the opinions of the competent parliamentary committees of the Chamber of Deputies and the Senate of the Republic are obtained on the draft legislative decrees for implementation. In this case, the draft legislative decrees are transmitted, after obtaining the other opinions required by law, to the Chamber of Deputies and the Senate of the Republic for their consideration.



they are given the opinion of the competent parliamentary committees.
After forty days from the date of transmission, the decrees are issued even in the absence of an opinion. If the deadline for the expression of the parliamentary opinion referred to in this paragraph or the different deadlines set forth in paragraphs 4 and 9 expire within thirty days preceding the expiration of the delegation deadlines set forth in paragraphs 1 or 5 or subsequently, the latter shall be extended by three months.

4. The draft legislative decrees implementing directives with financial implications shall be accompanied by the technical report referred to in Article 17, paragraph 3, of Law No. 196 of 31 December 2009. The opinion of the parliamentary committees responsible for financial matters shall also be required. If the Government does not intend to comply with the conditions formulated with reference to the need to ensure compliance with Article 81, paragraph 4, of the Constitution, it shall return the texts to the Chambers, accompanied by the necessary additional information, for the final opinions of the parliamentary committees responsible for financial matters, which must be expressed within twenty days.

5. Within twenty-four months of the date of entry into force of each of the legislative decrees referred to in paragraph 1, in compliance with the principles and guiding criteria established by the European delegation law, the Government may adopt, with the procedure indicated in paragraphs 2, 3 and 4, supplementary and corrective provisions to the legislative decrees issued pursuant to the aforementioned paragraph 1, without prejudice to the different deadline provided for in paragraph 6.

6. With the procedure referred to in paragraphs 2, 3, and 4, the Government may adopt supplementary and corrective provisions to legislative decrees issued pursuant to paragraph 1, in order to implement European Union delegated acts referred to in Article 290 of the Treaty on the Functioning of the European Union, which amend or supplement directives implemented by such legislative decrees. The supplementary and corrective provisions referred to in the first sentence shall be adopted within the deadline referred to in paragraph 5 or within a different deadline established by the European delegation law. The provisions of Article 36 for the implementation of European Union delegated acts that merely contain technical adjustments remain in effect.

7. The legislative decrees implementing the directives provided for by the European delegation law, adopted pursuant to Article 117, paragraph 5, of the Constitution, in matters falling within the legislative competence of the regions and autonomous provinces, shall apply under the conditions and according to the procedures set out in Article 41, paragraph 1.

8. Legislative decrees adopted pursuant to Article 33 and pertaining to matters within the legislative competence of the regions and autonomous provinces are issued under the conditions and according to the procedures set out in Article 41, paragraph 1.

9. When the Government does not intend to comply with the parliamentary opinions referred to in paragraph 3 regarding criminal sanctions contained in the draft legislative decrees implementing the directives, it shall retransmit the texts, with its observations and any amendments, to the Chamber of Deputies and the Senate of the Republic. After twenty days from the date of retransmission, the decrees shall be issued even in the absence of a new opinion.

«Art. 32 *(General principles and guidelines for delegation for the implementation of European Union law)* . — 1. Without prejudice to the specific principles and guidelines established by the European delegation law and in addition to those contained in the directives to be implemented, the legislative decrees referred to in Article 31 are informed by the following general principles and guidelines: *a)* the

administrations directly involved shall implement the legislative decrees with the ordinary administrative structures, according to the principle of maximum simplification of procedures and methods of organization and exercise of functions and services; *b)* for the purposes of better coordination with the regulations in force for the individual sectors affected

by the legislation to be implemented, the necessary modifications to the regulations themselves shall be introduced, including through regulatory reorganization and simplification with explicit indication of the repealed provisions, without prejudice to the procedures subject to administrative simplification or the matters subject to deregulation; *c)* the acts implementing European Union directives cannot provide for the introduction or maintenance of levels of regulation higher than the minimum levels

required by the directives themselves, pursuant to Article 14, paragraphs 24 -*bis* of Law No. 246 of 28 November 2005; *d)* outside the cases provided for by the criminal law in force, where necessary to ensure compliance with the provisions contained in the legislative decrees, administrative and criminal sanctions are provided for

Violations of the provisions of the decrees themselves. Criminal penalties, up to a fine of up to €150,000 and imprisonment of up to three years, are provided, alternatively or jointly, only in cases where the violations harm or jeopardize constitutionally protected interests. In such cases, the following are provided: a fine as an alternative to imprisonment for violations that jeopardize or damage the protected interest; and imprisonment combined with a fine for violations that cause particularly serious harm. In the aforementioned cases, in lieu of imprisonment and a fine, the alternative penalties set forth in Articles 53 et seq. of Legislative Decree No. 274 of August 28, 2000, and the related jurisdiction of the Justice of the Peace, may also be provided. The administrative sanction of a fine of no less than €150 and no more than €150,000 is provided for violations that harm or jeopardize interests other than those indicated in this letter. Within the minimum and maximum limits provided, the sanctions indicated in this letter are determined in their amount by taking into account the different potential harm to the protected interest that each violation theoretically presents, the specific personal characteristics of the offender, including those that impose particular duties of prevention, control, or supervision, as well as the financial advantage that the violation may bring to the offender or to the person or entity in whose interest he or she acts. Where necessary to ensure compliance with the provisions contained in the legislative decrees, additional administrative sanctions are also provided for: suspension of up to six months and, in the most serious cases, permanent deprivation of powers and rights deriving from administrative measures, as well as additional criminal sanctions within the limits established by the Criminal Code. To the same end, the mandatory confiscation of items used or intended to commit the administrative offense or crime provided for by the same legislative decrees is provided for, within the limits established by Article 240, paragraphs three and four, of the Criminal Code and Article 20 of Law No. 689 of November 24, 1981, and subsequent amendments. Within the penalty limits indicated in this letter, additional penalties are also provided, identical to those already imposed by existing laws for homogeneous violations of the same nature and of equal offensiveness as violations of the provisions of the legislative decrees. In the matters referred to in Article 117, paragraph four, of the Constitution, administrative penalties are determined by the regions; *e)* the transposition of directives or the implementation of other European Union acts that amend previous directives or acts already implemented by law or legislative decree shall be carried out, if the amendment does not entail an expansion of the regulated subject matter, by making the corresponding amendments to the law or legislative decree implementing the directive or other amended act; *f)* in drafting the legislative decrees referred to in Article 31, any amendments to the European Union directives that may have occurred up to the time of the exercise of the delegation shall be taken into account;

g) when there are overlaps in responsibilities between different administrations or in any case the responsibilities of multiple state administrations are involved, the legislative decrees identify, through the most appropriate forms of coordination, respecting the principles of subsidiarity, differentiation, adequacy and loyal cooperation and the responsibilities of the regions and other territorial entities, the procedures to safeguard the unity of decision-making processes, transparency, speed, effectiveness and cost-effectiveness in administrative action and the clear identification of the responsible parties; *h)* where different transposition deadlines are not an obstacle, directives that concern the same matters or that

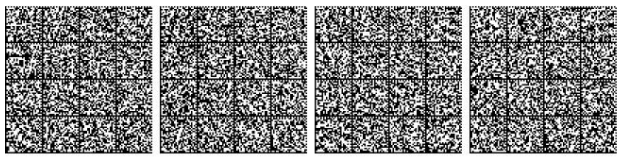
in any case involve amendments to the same legislative acts are implemented with a single legislative decree; *i)* equal treatment of Italian citizens with respect to citizens of other Member States of the European Union is ensured and in any case unfavorable

treatment of Italian citizens cannot be envisaged.

— Article 3 of Law No. 15 of 21 February 2024 (Delegation to the Government for the transposition of European directives and the implementation of other European Union legislative acts - European Delegation Law 2022-2023), published in the *Official Journal* No. 46 of 24 February 2024, is reported: «Art. 3. *(Principles and guiding criteria*

for the exercise of the delegation for the transposition of Directive (EU) 2022/2555, relating to 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 (NIS2 Directive)).

— 1. In exercising the delegation for the transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December



2022, the Government, after consulting the National Cybersecurity Agency, observes, in addition to the general principles and guidelines set out in Article 32 of Law No. 234 of 24 December 2012, the following specific principles and guidelines: *a)* identify the criteria by which a

public body can be considered a public administration for the purposes of applying the provisions of Directive (EU) 2022/2555, also considering the possibility of applying the same directive to municipalities and provinces according to the principles of graduality, proportionality and adequacy; *b)* exclude from the scope of the provisions of Directive (EU) 2022/2555 public administration bodies operating in the sectors

referred to in Article 2, paragraph 7, of the same directive, including security intelligence bodies to which the provisions of Law No. 124 of 3 August 2007 apply;

c) make use of the option referred to in Article 2, paragraph 8, of Directive (EU) 2022/2555, providing that with one or more decrees of the President of the Council of Ministers, adopted on the proposal of the competent administrations, specific subjects who carry out activities in the sectors indicated therein or who provide services exclusively to the public administration bodies referred to in Article 2, paragraph 7, of the same directive are exempted;

(d) confirm the distinction between the National Cybersecurity Agency, as the competent national authority and point of contact, pursuant to Article 8 of Directive (EU) 2022/2555, and the sector authorities operating in the areas referred to in Annexes I and II to the same Directive;

e) in relation to the establishment of the Computer Security Incident Response Team (CSIRT), pursuant to Article 10 of Directive (EU) 2022/2555, confirm the provisions of Article 8 of Legislative Decree no. 65 of 18 May 2018, regarding the establishment of the CSIRT Italy, as well as expand the provisions of the same legislative decree by providing for collaboration between all public structures with Computer Emergency Response Team (CERT) functions involved in the event of malicious cybersecurity events; *f)* provide for a transitional regime for entities already subject to the provisions of Legislative Decree no. 65 of 18 May

2018, implementing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, ensuring appropriate deadlines for adaptation, for the purpose of better application of the provisions of Directive (EU) 2022/2555; *g)* provide mechanisms that allow for the registration of essential and important entities, as referred to in Article 3 of Directive (EU) 2022/2555, for the communication of the data required by paragraph 4

of the same Article 3, including entities managing services connected or instrumental to the activities covered by the provisions of the same Directive relating to the cultural sector; *h)* in relation to the measures referred to in Article 21, paragraph 2, of Directive (EU) 2022/2555, provide for the identification, through the use of flexible tools suited to rapid technological development, of the technologies necessary to ensure the effective activation of these

measures. The administrative authority identified as responsible for this procedure shall also ensure the updating of the adopted tools; *i)* introduce into current legislation, including criminal law, the necessary amendments to ensure the correct transposition into national law of the provisions of Directive (EU) 2022/2555 regarding coordinated disclosure of vulnerabilities;

(l) define the responsibilities of the Agency for Digital Italy and the National Cybersecurity Agency in relation to the activities provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014; (m) identify objective and proportionate criteria for

the purposes of applying the disclosure requirements referred to in Article 23, paragraph 2, of Directive (EU) 2022/2555;

n) review the sanctioning system and the supervisory and enforcement system, in particular: 1)

providing for effective, proportionate and dissuasive sanctions with respect to the seriousness of the violation of the obligations arising from Directive (EU) 2022/2555, even in derogation from the criteria and limits set out in Article 32, paragraph 1, letter *d)* , of Law No. 234 of 24 December 2012 and Law No. 689 of 24 November 1981, introducing instruments to deflate litigation, such as formal notices to comply; 2) providing that the proceeds deriving from the imposition

of sanctions are paid into the State budget to be reallocated to the appropriate chapter of the Ministry of Economy and Finance's expenditure estimates, pursuant to Article 18 of Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021, to increase the budget of the National Cybersecurity Agency;

o) ensure the best coordination between the provisions adopted pursuant to this Article for the transposition of Directive (EU) 2022/2555, the provisions adopted pursuant to Article 5 of this Law for the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, as well as the provisions of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 and those adopted pursuant to Article 16 of this Law for the adaptation to the latter and for the transposition of Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022; *p)* make all the amendments and additions to the legislation in force necessary to ensure coordination with the provisions issued in implementation of this Article.».

— Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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 is published in the OJEU No 17 of 27 December 2022, Series L.

— The Commission Communication of 13 September 2023 on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 is published in OJEU No. 328 of 18 September 2023, C series; — Directive 2002/58/EC of the European Parliament and of the

Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) is published in OJEU No. 201 of 31 July 2002, L series;

— Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC is published in the OJEU of 28 August 2014 No 257, Series L; — Regulation (EU) 2024/1183 of the European Parliament and of the

Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European framework for a digital identity is published in the OJEU of 30 April 2024, Series L; — Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for

Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 ('Cybersecurity Regulation') is published in the OJEU of 7 June 2019 151 series L;

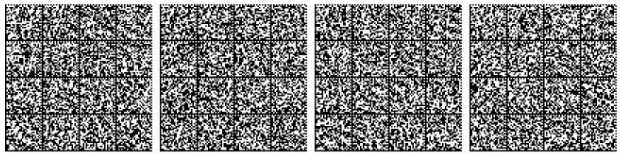
— Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises is published in the Official Journal of the European Union of 20 May 2003, No. 124, Series L.

— Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA is published in the Official Journal of the European Union of 14 August 2013; — Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14

December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 is published in the OJEU of 27 December 2022 No 133 series L; — Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU,

2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector is published in the OJEU of 27 December 2022 No 333;

— Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC is published in the OJEU of 27 December 2022 No 333, series L;



— Articles 1 and 2 of Legislative Decree No. 118 of 23 June 2011 (Provisions regarding the harmonization of accounting systems and budget formats of the Regions, local authorities and their bodies, pursuant to Articles 1 and 2 of Law No. 42 of 5 May 2009), published in the *Official Journal* No. 172 of 26 July 2011, are reported below: «Art. 1 *(Object and scope of application)* .

— 1. Pursuant to Article 117, paragraph 2, letter *e)* , of the Constitution, this Title and Title III regulate the harmonization of the accounting systems and budget formats of the Regions, except where Title II provides otherwise, with particular reference to the situation referred to in Article 19, paragraph 2, letter *b)* , of the local authorities referred to in Article 2 of Legislative Decree No. 267 of 18 August 2000, and of their instrumental bodies and organizations, excluding the bodies referred to in Title II of this decree. Starting from 1 January 2015, any regional legislative provisions incompatible with this decree shall cease to be effective.

2. For the purposes of this decree:

a) instrumental entities means the entities referred to in Article 11 - divided into the types , defined in correspondence with the missions of the *third* budget;

b) Instrumental bodies of regions and local authorities are their organizational branches, including those at the territorial level, with managerial and accounting autonomy and without legal personality. The off-budgetary managements authorized by law and the institutions referred to in Article 114, paragraph 2, of Legislative Decree No. 267 of August 18, 2000, are instrumental bodies. The instrumental bodies are classified according to the types defined in the budget missions.

3.

4.

5. For the bodies involved in the management of healthcare expenditure financed with resources allocated to the National Health Service, as identified in Article 19, the provisions set out in Title II shall apply.»

«Art. 2 *(Adoption of homogeneous accounting systems)* . — 1. The Regions and local authorities referred to in Article 2 of Legislative Decree No. 267 of 18 August 2000 shall adopt financial accounting, which they shall supplement, for information purposes, with an economic-patrimonial accounting system, ensuring the uniform recording of management events from both a financial and an economic-patrimonial perspective.

2. The instrumental bodies of the administrations referred to in paragraph 1 that adopt financial accounting shall, for information purposes, combine it with an economic-patrimonial accounting system, ensuring the unitary recording of management events, both from a financial and an economic-patrimonial perspective.

3. The local government institutions referred to in Article 114 of Legislative Decree No. 267 of 18 August 2000 and the other instrumental bodies of the public administrations referred to in paragraph 1 shall adopt the same accounting system as the administration of which they are a part.

4.»

— Article 19 of Legislative Decree No. 83 of June 22, 2012 (Urgent measures for the growth of the country) is reported, converted, with amendments, by Law No. 134 of August 7, 2012, published in the *Official Journal.*
June 26, 2012, no. 147, SO: — 1.

«Art. 19 *(Establishment of the Agency for Digital Italy)* . establishes the Agency for Digital Italy, subject to the supervision of the President of the Council of Ministers or the Minister delegated by him.

2. The Agency operates on the basis of principles of organizational, technical-operational, and managerial autonomy, transparency, and cost-effectiveness, and pursues the objectives of effectiveness, efficiency, impartiality, simplification, and citizen and business participation. For any matters not covered by this decree, Articles 8 and 9 of Legislative Decree No. 300 of July 30, 1999, shall apply to the Agency.

— Article 3 of Law No. 15 of 21 February 2024 (Delegation to the Government for the transposition of European directives and the implementation of other acts of the European Union - European Delegation Law 2022-2023), published in the *Official Journal* No. 46 of 24 February 2024, is reported: «Art. 3 *(Principles and guiding criteria for the exercise of the delegation for the transposition of Directive (EU) 2022/2555, relating to 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 (NIS2 Directive)).*

— 1. In exercising the delegation for the transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, the Government, after consulting the National Cybersecurity Agency, observes, in addition to the general principles and guidelines referred to in Article 32 of Law No. 234 of 24 December 2012, also the following specific principles and guidelines: *a)* identify

the criteria on the basis of which a public body can be considered a public administration for the purposes of applying the provisions of Directive (EU) 2022/2555, also considering the possibility of applying the same directive to municipalities and provinces according to the principles of graduality, proportionality and adequacy; *b)* exclude from the scope of application of the provisions of Directive (EU) 2022/2555

public administration bodies operating in the sectors referred to in Article 2, paragraph 7, of the same directive, including security intelligence bodies to which the provisions of Law No. 124 of 3 August 2007 apply;

c) make use of the option referred to in Article 2, paragraph 8, of Directive (EU) 2022/2555, providing that with one or more decrees of the President of the Council of Ministers, adopted on the proposal of the competent administrations, specific subjects who carry out activities in the sectors indicated therein or who provide services exclusively to the public administration bodies referred to in Article 2, paragraph 7, of the same directive are exempted;

(d) confirm the distinction between the National Cybersecurity Agency, as the competent national authority and point of contact, pursuant to Article 8 of Directive (EU) 2022/2555, and the sector authorities operating in the areas referred to in Annexes I and II to the same Directive;

e) in relation to the establishment of the Computer Security Incident Response Team (CSIRT), pursuant to Article 10 of Directive (EU) 2022/2555, confirm the provisions of Article 8 of Legislative Decree no. 65 of 18 May 2018, regarding the establishment of the CSIRT Italy, as well as expand the provisions of the same legislative decree by providing for collaboration between all public structures with Computer Emergency Response Team (CERT) functions involved in the event of malicious cybersecurity events; *f)* provide for a transitional regime for entities already subject to the provisions of Legislative Decree no. 65 of 18 May 2018,

implementing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, ensuring appropriate deadlines for adaptation, for the purpose of better application of the provisions of Directive (EU) 2022/2555; *g)* provide mechanisms that allow for the registration of essential and important entities, as referred to in Article 3 of Directive (EU) 2022/2555, for the communication of the data required by paragraph 4 of the same Article 3, including

entities managing services connected or instrumental to the activities covered by the provisions of the same Directive relating to the cultural sector; *h)* in relation to the measures referred to in Article 21, paragraph 2, of Directive (EU) 2022/2555, provide for the identification, through the use of flexible tools suited to rapid technological development, of the technologies necessary to ensure the effective activation of these measures. The administrative

authority identified as responsible for this procedure shall also ensure the updating of the adopted tools; *i)* introduce into current legislation, including criminal law, the necessary amendments to ensure the correct transposition into national law of the provisions of Directive (EU) 2022/2555 regarding coordinated disclosure of vulnerabilities;

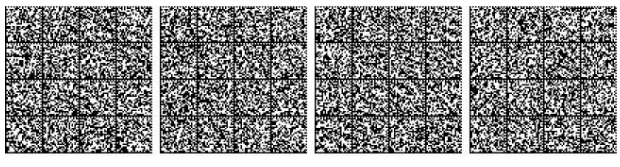
(l) define the responsibilities of the Agency for Digital Italy and the National Cybersecurity Agency in relation to the activities provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014; (m) identify objective and proportionate criteria for

the purposes of applying the disclosure requirements referred to in Article 23, paragraph 2, of Directive (EU) 2022/2555;

n) review the sanctions system and the supervisory and enforcement system, in particular: 1) providing for

effective, proportionate and dissuasive sanctions with respect to the seriousness of the violation of the obligations arising from Directive (EU) 2022/2555, even in derogation from the criteria and limits set out in Article 32, paragraph 1, letter *d)* , of Law No. 234 of 24 December 2012 and Law No. 689 of 24 November 1981, introducing instruments to deflate litigation, such as formal notices to comply; 2) providing that the proceeds deriving from the imposition of sanctions are paid

into the State budget to be reassigned to the appropriate chapter of the expenditure forecast of the Ministry of Economy and Finance, pursuant to Article 18 of the Directive.



Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021, to increase the budget of the National Cybersecurity Agency; *o)* ensure the best coordination between the provisions

adopted pursuant to this Article for the transposition of Directive (EU) 2022/2555, the provisions adopted pursuant to Article 5 of this Law for the transposition of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, as well as the provisions of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 and those adopted pursuant to Article 16 of this Law for the adaptation to the latter and for the transposition of Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022; *p)* make all the amendments and additions to the legislation in force necessary to ensure coordination with the provisions issued in implementation of this Article.».

— The text of Article 8 of Legislative Decree No. 281 of 28 August 1997 (Definition and expansion of the powers of the Permanent Conference for relations between the State, the regions and the autonomous provinces of Trento and Bolzano and unification, for matters and tasks of common interest to the regions, provinces and municipalities, with the State-Cities and Local Authorities Conference) published in the *Official Journal* No. 202 of 30 August 1997 is reported: «Art. 8. *(State-Cities and Local Authorities Conference and Unified Conference)* .

— 1. The State-Cities and Local Authorities Conference is unified with the State-Regions Conference for matters and tasks of common interest to the regions, provinces, municipalities, and mountain communities.

2. The State-Cities and Local Authorities Conference is chaired by the Prime Minister or, by his delegation, by the Minister of the Interior or the Minister for Regional Affairs in matters within their respective areas of competence. It also includes the Minister of the Treasury, Budget and Economic Planning, the Minister of Finance, the Minister of Public Works, the Minister of Health, the President of the National Association of Italian Municipalities (ANCI), the President of the Union of Italian Provinces (UPI), and the President of the National Union of Mountain Municipalities, Communities and Authorities (UNCEM). It also includes fourteen mayors designated by ANCI and six provincial presidents designated by UPI. Of the fourteen mayors designated by ANCI, five represent the cities identified in Article 17 of Law No. 142 of June 8, 1990. Other members of the Government, as well as representatives of state, local, or public administrations, may be invited to the meetings.

3. The State-City and Local Authorities Conference is convened at least every three months, and in any case in all cases the president deems it necessary or when requested by the president of ANCI, UPI or UNCEM.

4. The Unified Conference referred to in paragraph 1 is convened by the President of the Council of Ministers. The meetings are chaired by the President of the Council of Ministers or, upon his delegation, by the Minister for Regional Affairs or, if such a mandate is not conferred, by the Minister of the Interior.

Notes to Article 1:

— Articles 9 and 10 of Legislative Decree No. 82 of June 14, 2021 (Urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency), published in the *Official Journal* No. 140 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021 (published in the *Official Journal* No. 185 of August 4, 2021) are reported: «Art. 9 *(Tasks of the Cybersecurity Unit)* .

— 1. For the purposes set out in Article 8, the Cybersecurity Unit carries out the following tasks: *a)* it can formulate

proposals for initiatives regarding the country's cybersecurity, also within the framework of the relevant international context;

b) promotes, on the basis of the directives referred to in Article 2, paragraph 2, the programming and operational planning of the response to cyber crisis situations by the administrations and private operators involved and the development of the necessary inter-ministerial coordination procedures, in conjunction with civil defense and civil protection planning, also within the framework of the provisions of Article 7 *-bis,* paragraph 5, of Legislative Decree no. 174 of 30 October 2015, converted, with amendments, by Law no. 198 of 11 December 2015;

c) promotes and coordinates the conduct of inter-ministerial exercises, or national participation in international exercises involving the simulation of cyber events in order to increase the country's resilience; *d)* evaluates and promotes, in coordination with the administrations responsible for specific

cybersecurity aspects, information-sharing procedures, including with interested private operators, for the purpose of disseminating alerts relating to cyber events and for crisis management; *e)* acquires, including through CSIRT Italy, communications regarding cases of breaches or attempted breaches of security or loss of integrity that are

significant for the proper functioning of networks and services from the information bodies referred to in Articles 4, 6, and 7 of Law No. 124 of 3 August 2007, from the police forces, and in particular, from the body of the Ministry of the Interior referred to in Article 7 *-bis.*

of Legislative Decree No. 144 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005, by the structures of the Ministry of Defence, as well as by the other administrations that make up the Nucleus and by the intervention groups for computer emergencies (Computer Emergency Response Team - CERT) established pursuant to current legislation;

f) receives incident notifications from CSIRT Italia pursuant to the provisions in force; *g)* assesses whether

the events referred to in letters *e)* and *f)* are of such a size, intensity, or nature that they cannot be addressed by the individual competent administrations on an ordinary basis, but require coordinated decisions at an inter-ministerial level, and in this case promptly informs the President of the Council of Ministers, or the Delegated Authority, where established, of the current situation and the performance of the coordination and coordination activities referred to in Article 10, in the composition provided for therein.».

«Art. 10 *(Management of crises involving cybersecurity aspects)* .

— 1. In crisis situations involving cybersecurity aspects, in cases where the President of the Council of Ministers convenes the CISR to manage such crisis situations, the Minister with responsibility for technological innovation and digital transition and the Director General of the Agency are called to participate in the Committee's meetings.

2.

3. In cybercrisis situations, the Unit is supplemented, as needed, by a representative from each of the Ministry of Health and the Ministry of the Interior - Department of Firefighters, Public Rescue, and Civil Defense, also representing the Interministerial Technical Commission for Civil Defense. These representatives are authorized to make decisions that affect their respective administrations. Members may be accompanied by other officials from their own administrations to attend meetings. Representatives of other administrations, including local ones, and entities, who are also authorized to make decisions, and of other interested public or private entities, may be invited to attend the same meetings. No compensation, attendance fees, expense reimbursements, or other emoluments, however denominated, are provided for participation. 4. It is the task of the Unit, in its composition for crisis management, referred to in paragraph 3, to ensure that the reaction and stabilization activities under the responsibility of the various administrations and bodies with

respect to cyber crisis situations are carried out in a coordinated manner in accordance with the provisions of Article 9, paragraph 1, letter *b)* .

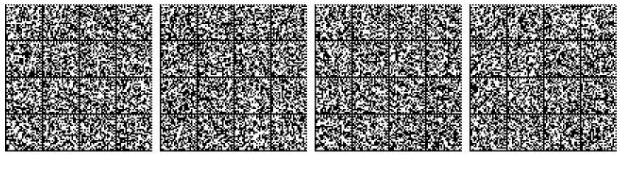
5. The Unit, in order to carry out its functions and without prejudice to the provisions of Article 7 *-bis,* paragraph 5, of Legislative Decree No.,174 of 30 October 2015, converted, with amendments, by Law No. 198 of 11 December 2015:

a) keeps the Prime Minister, or the Delegated Authority, where established, constantly informed of the ongoing crisis, preparing updated status reports; *b)* ensures coordination for the implementation at the inter-ministerial level

of the Prime Minister's decisions to overcome the crisis; *c)* collects all data relating to the crisis; *d)* prepares reports and provides information on the crisis and transmits them to the interested

public and private entities;

e) participates in European cyber crisis management mechanisms, also ensuring connections aimed at crisis management with counterpart bodies in other States, NATO,



of the European Union or of international organizations of which Italy is a member.».

— For references to Directive (EU) 2022/2555 (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 2 Directive), see the notes to the preamble.

Notes to Article 2:

— Articles 1, as amended by this decree, as well as 5 and 8, of the aforementioned Legislative Decree no. 82 of 14 June 2021, converted, with amendments, by Law no. 109 of 4 August 2021, are reported

below: «Art. 1 *(Definitions)* . 1. For the purposes of this decree, it is understood that For:

a) cybersecurity, the set of activities, without prejudice to the powers set forth in Law No. 124 of 3 August 2007 and the obligations deriving from international treaties, necessary to protect networks, information systems, IT services and electronic communications from cyber threats, ensuring their availability, confidentiality and integrity and guaranteeing their resilience, also for the purposes of protecting national security and national interests in cyberspace; *b)* national resilience in cyberspace, the activities aimed at preventing harm to national security as defined in Article 1,

paragraph 1, letter *f)* , of the regulation referred to in Prime Ministerial Decree No. 131 of 30 July 2020;

c) Perimeter Decree-Law means Legislative Decree No. 82 of 14 June 2021, converted, with amendments, by Law No. 133 of 18 November 2019, containing urgent provisions regarding the perimeter of national cyber security and the regulation of special powers in sectors of strategic importance; d) *NIS Legislative Decree means the legislative decree*

transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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 ;

e) national cybersecurity strategy, the strategy *referred to in Article 9* of the NIS Legislative Decree.» — 1. «Art. 5 *(National Cybersecurity Agency)* . The

National Cybersecurity Agency, referred to for the purposes of this decree as the «Agency», with headquarters in Rome, is hereby established to protect national interests in the field of cybersecurity.

2. The Agency has legal personality under public law and enjoys regulatory, administrative, patrimonial, organizational, accounting, and financial autonomy, within the limits set forth in this decree. The President of the Council of Ministers and the Delegated Authority, where established, shall avail themselves of the Agency to exercise the powers set forth in this decree.

3. The Director General of the Agency is appointed from among individuals belonging to one of the categories referred to in Article 18, paragraph 2, of Law No. 400 of 23 August 1988, who possess documented high-level experience in managing innovation processes. The terms of office of the Director General and Deputy Director General have a maximum duration of four years and are renewable, with subsequent provisions, for a maximum total term of an additional four years. The Director General and Deputy Director General, if they come from public administrations as per Article 1, paragraph 2, of Legislative Decree No. 165 of 30 March 2001, are placed on secondment or in a position of command or other similar position, according to their respective regulations. Pursuant to this decree, the Director General of the Agency is the direct report of the President of the Council of Ministers and the Delegated Authority, where established, and is hierarchically and functionally superior to the Agency's staff. The Director General is the legal representative of the Agency.

4. The Agency's activity is regulated by this decree and by the provisions whose adoption is foreseen by it.

5. The Agency may request, also on the basis of specific agreements and in compliance with the areas of specific competence, the collaboration of other state bodies, other administrations, the Armed Forces, the police forces or public bodies in carrying out its institutional tasks.

6. COPASIR, pursuant to the provisions of Article 31, paragraph 3, of Law No. 124 of 3 August 2007, may request a hearing with the Director General of the Agency on matters within its jurisdiction.

«Art. 8 *(Cybersecurity Unit)* . — 1. The Cybersecurity Unit is permanently established within the Agency to support the President of the Council of Ministers in matters of cybersecurity, for aspects relating to prevention and preparedness for possible crisis situations and for the activation of alert procedures.

2. The Cybersecurity Unit is chaired by the Director General of the Agency or, by his delegation, by the Deputy Director General and is composed of the Military Advisor to the President of the Council of Ministers, a representative each of the DIS, the External Information and Security Agency (AISE), pursuant to Article 6 of Law No. 124 of 3 August 2007, the Internal Information and Security Agency (AISI), pursuant to Article 7 of Law No. 124 of 2007, each of the Ministries represented in the CIC, and the Civil Protection Department of the Presidency of the Council of Ministers. For matters relating to the handling of classified information, the Unit is supplemented by a representative of the Central Office for Secrecy pursuant to Article 9 of Law No. 124 of 2007.

3. The members of the Committee may be assisted at meetings by other representatives of their respective administrations, depending on the matters being discussed. Depending on the topics of the meetings, representatives of other administrations, universities, or research institutions and organizations, as well as private operators interested in cybersecurity, may also be invited to participate.

4. The Nucleus may be convened in a restricted composition with the participation of representatives of the administrations and interested parties only, also with regard to the crisis management tasks referred to in Article 10.

4.1. In relation to specific issues of particular relevance concerning the tasks referred to in Article 9, paragraph 1, letter *a)* , the Unit may be convened in the composition referred to in paragraph 4 of this Article, extended from time to time to the participation of a representative of the National Anti-Mafia and Anti-Terrorism Directorate, the Bank of Italy, or one or more operators referred to in Article 1, paragraph 2 *-bis* of the Perimeter Decree, as well as any other subjects interested in the same issues. The administrations and subjects convened participate in the aforementioned meetings at the top level. 4 *-bis*

· The members of the Nucleus are not entitled to compensation, attendance fees, reimbursements of expenses or other emoluments of any kind.».

— For Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 see notes to the premises.

— For Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act'), see the footnotes to the preamble.

— The text of Article 2, paragraph 1, letter *vv)* of Legislative Decree 1 August 2003, n. 259 (Electronic Communications Code) published in the *Official Journal* 15 September 2003, n. 214 «Art. 2 *(Definitions)* .

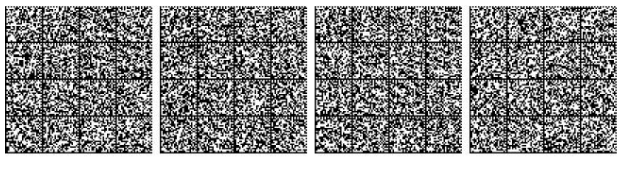
— 1. For the purposes of this decree, it is understood that For:

(Omitted)

vv) electronic communications networks: transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity and, where applicable, switching or routing equipment and other resources, including non-active network elements, which enable the transmission of signals by wire, by radio, by optical fibre or by other electromagnetic means, including satellite networks, mobile and fixed networks (circuit-switched and packet-switched, including the Internet), systems for the cable transport of electric power, insofar as they are used to transmit signals, networks used for radio and television broadcasting and cable television networks, regardless of the type of information transported;

(Omitted).».

— Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/
EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council is published in the OJEU of 14 November 2012 No 316, series L.



— Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 is published in the OJEU of 17 September 2015 No. 241, series L.

— Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC is published in the Official Journal of the European Union of 28 July 2014 No. 257, Series L.

— Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC and Directives 97/7/EC, 98/27/EC and 2002/65/EC
EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') is published in the OJEU of 11 June 2005 No 149, Series L.

— Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 is published in the OJEU of 17 December 2018 No 321, Series L.

Notes to Article 3:

— The Commission Recommendation of 6 May 2003,
No. 361 is published in the Official Journal of the European Union of 20 May 2003, No. 124, Series L.

— The text of Article 1 of Law No. 196 of 31 December 2009 (Public Accounting and Finance Law) published in the Official Journal No. 303 of 31 December 2009, SO is reported below: «Art. 1 *(Coordination*

principles and scope of reference) .

1. Public administrations contribute to the pursuit of public finance objectives defined at the national level in accordance with the procedures and criteria established by the European Union and share the resulting responsibilities. Contribution to the pursuit of these objectives is achieved according to the fundamental principles of harmonization of public budgets and coordination of public finances.

2. For the purposes of applying the provisions on public finance, public administrations shall mean, for the year 2011, the bodies and subjects indicated for statistical purposes in the list included in the press release of the National Institute of Statistics (ISTAT) dated 24 July 2010, published on the same date in the *Official Journal* of the Italian Republic no. 171, as well as, starting from the year 2012, the bodies and subjects indicated for statistical purposes by the aforementioned Institute in the list included in the press release of the same Institute dated 30 September 2011, published on the same date in the *Official Journal* of the Italian Republic no. 228, and subsequent updates pursuant to paragraph 3 of this article, carried out on the basis of the definitions set out in the specific European Union regulations, the independent Authorities and, in any case, the administrations referred to in Article 1, paragraph 2, of Legislative Decree no. 30 March 2001. 165, and subsequent amendments.

3. The survey of public administrations referred to in paragraph 2 is carried out annually by ISTAT with its own provision and published in the *Official Journal* by September 30.

4. The provisions of this law and the related legislative decrees constitute fundamental principles of the coordination of public finances pursuant to Article 117 of the Constitution and are aimed at protecting the economic unity of the Italian Republic, pursuant to Article 120, second paragraph, of the Constitution.

5. The provisions of this law apply to the regions with special statutes and to the autonomous provinces of Trento and Bolzano in compliance with the provisions of the relevant statutes."

— For the purposes of the definition of essential service operator, the text of Articles 3 and 4 of Legislative Decree No. 65 of 18 May 2018 (Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) published in the Official Journal of 9 June 2018, No. 132, SO: «Art. 3 *(Definitions)* .

— 1. For the purposes of this decree, it is understood that For:

a) competent national NIS authority, the single national authority competent for network and information systems security, referred to in Article 7, paragraph 1; a *-bis)* sector authorities, the authorities referred

to in Article 7, paragraph 1, letters *a)* to *e) ; b)* CSIRT, the computer security incident response

group, referred to in Article 8;

(c) single point of contact, the body responsible at national level for coordinating issues relating to the security of network and information systems and cross-border cooperation at European Union level;

d) law enforcement authority, the central body of the Ministry of the Interior for the security and regularity of telecommunications services, referred to in Article 7 *-bis* of Legislative Decree No. 144 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005; *e)* network and information system:

1) an electronic communications network pursuant to Article 1, paragraph 1, letter *dd) ,* of Legislative Decree no. 259 of 1 August 2003;

2) any device or group of interconnected or linked devices, one or more of which perform, pursuant to a program, automatic processing of digital data; 3) digital data stored, processed, retrieved or transmitted

via networks or devices referred to in points 1) and 2), for their operation, use, protection and maintenance; *f)* network and information systems security, the ability of a network and information systems to

resist, at a given level of confidentiality, any action that compromises the availability, authenticity, integrity or confidentiality of the data stored or transmitted or processed and of the related services offered or accessible via such network or information systems; *g)* operator of essential services, whether public or private, of the type referred to in Annex II, which meets the criteria set out in Article 4, paragraph 2;

(h) digital service means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 of a type listed in Annex III; *(i)* digital service provider means any legal person

who
provides a digital service;

l) incident, any event with a real detrimental effect on the security of the network and information systems; *m)* incident handling, all

procedures necessary for the identification, analysis, and containment of an incident and intervention in the event of an incident;

(n) risk, any reasonably identifiable circumstance or event with potential detrimental effects on the security of network and information systems; *(o)* representative, the natural or legal person

established in the European Union expressly designated to act on behalf of a digital service provider that is not established in the European Union, to whom the competent NIS authority or the National CSIRT may turn in place of the digital service provider, with regard to the latter's obligations under this decree; (p) standard, a standard pursuant to Article 2, first paragraph, number 1), of Regulation (EU) No. 1025/2012;

q) specification, a technical specification within the meaning of Article 2, pri- paragraph 4), of Regulation (EU) No 1025/2012;

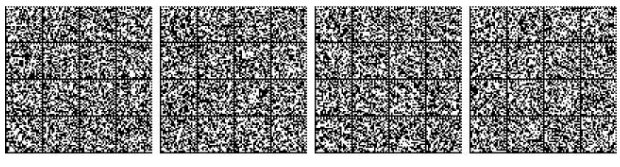
r) Internet Exchange Point (IXP) means a network infrastructure that allows the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic; an IXP provides interconnection only to autonomous systems; an IXP does not require, nor otherwise alter or interfere with, Internet traffic passing between any pair of participating autonomous systems to pass through a third autonomous system;

s) domain name system (DNS), is a distributed, hierarchical naming system in a network that forwards requests for domain names;

t) DNS service provider, a person who provides services
DNS on the Internet;

u) top-level domain name registry, an entity that administers and operates the registration of Internet domain names within a specific top-level domain (TLD);

(v) online marketplace, a digital service that allows consumers or professionals, as defined respectively in Article 141, paragraph 1, letters a) and b), of Legislative Decree no. 206 of 6 September 2005, to conclude online sales or service contracts with professionals either on the online marketplace's website or on the website of a professional who uses the IT services provided by the online marketplace;



z) online search engine, a digital service that allows the user to search, in principle, all websites or websites in a particular language on the basis of a query on any topic in the form of a keyword, phrase or other input, and provides links where information relating to the requested content can be found ;

cloud computing service, a digital service that provides access to a scalable and elastic set of shareable computing resources.»

Of

«Art. 4 *(Identification of essential service operators)* . — 1. By 9 November 2018, the competent NIS authorities shall, through their own provisions, identify for each sector and subsector referred to in Annex II, the operators of essential services with an establishment in the national territory.

Operators providing healthcare services are identified by decree of the Minister of Health, in agreement with the Permanent Conference for Relations between the State, the Regions, and the Autonomous Provinces of Trento and Bolzano. Operators supplying and distributing water intended for human consumption are identified by decree of the Minister of the Environment, Land, and Sea, in agreement with the Permanent Conference for Relations between the State, the Regions, and the Autonomous Provinces of Trento and Bolzano.

2. The criteria for identifying essential service operators are as follows: *a)* an

entity provides a service that is essential for the maintenance of essential social and/or economic activities;

b) the provision of that service depends on the network and information systems; *c)* an

incident would have significant adverse effects on the provision of that service.

3. In addition to the criteria indicated in paragraph 2, the identification of essential service operators shall take into account the documents produced in this regard by the Cooperation Group referred to in Article 10.

4. For the purposes of paragraph 1, before adopting the measures provided for by the same provision, if a subject provides a service referred to in paragraph 2, letter *a)* , on the national territory and in another Member State or States of the European Union, the competent NIS authorities shall consult the competent authorities of the other Member States.

5. A national list of essential service operators is established at the Ministry of Economic Development. The Ministry of Economic Development forwards this list to the single point of contact and to the body of the Ministry of the Interior for the security and regularity of telecommunications services, referred to in Article 7 *-bis* of Legislative Decree No. 144 of July 27, 2005, converted, with amendments, by Law No. 155 of July 31, 2005.

6. The list of essential service operators identified pursuant to paragraph 1 shall be reviewed and, where appropriate, updated on a regular basis, and at least every two years after 9 May 2018, in the following manner:

a) the sector authorities, in relation to the sectors under their jurisdiction, propose to the competent national authority NIS the changes to the list of essential service operators, according to the criteria set out in paragraphs 2 and 3;

b) the proposals are evaluated and, where necessary, supplemented, in agreement with the sector authorities, by the competent national authority (NIS), which, through its own provisions, provides for changes to the list of essential service operators, also communicating these changes, in relation to the sectors under its jurisdiction, to the sector authorities.

7. By 9 November 2018, and every two years thereafter, the single point of contact shall transmit to the European Commission the information necessary for the evaluation of the implementation of this Decree, in particular the consistency of the approach regarding the identification of operators of essential services.

8. The information referred to in paragraph 7 shall include at least:

(a) national measures allowing for the identification of operators of essential services; *(b)*

the list of services referred to in paragraph 2; *(c)*

the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector; *(d)* the thresholds, where they exist, for

determining the relevant level of provision with reference to the number of users dependent on that service referred to in Article 5, paragraph 1, letter *a)* , or to the importance of that service.

particular operator of essential services referred to in Article 5, paragraph 1, letter *f)* .».

Notes to Article 4:

— The text of Article 6 of Legislative Decree No. 231 of 21 November 2007 (Implementation of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and of Directive 2006/70/EC containing implementing measures) published in the Official Journal of 14 December 2007, No. 290, SO is reported below:

«Art. 6 *(Financial Intelligence Unit)* . — 1. The Financial Intelligence Unit for Italy (UIF), established at the Bank of Italy, is autonomous and operationally independent. In implementation of this principle, the Bank of Italy regulates its organisation and functioning by regulation, including the confidentiality of the information acquired, allocating to it the financial means and resources suitable for ensuring the effective pursuit of its institutional purposes. Article 24, paragraph 6- *bis* of Law No. 262 of 28 December 2005 applies to the UIF and its staff. (41)

,

2. The Director of the UIF, who is independently responsible for its management, is appointed by a provision of the Board of Directors of the Bank of Italy, upon proposal of the Governor of the Bank of Italy, from among individuals with adequate integrity, professionalism, and knowledge of the financial system. The term of office is five years and may be renewed only once.

3. For the effective performance of the tasks established by law and international obligations, the UIF has established a Committee of Experts, comprising the Director and four members, each with adequate integrity and professionalism. The members of the Committee are appointed, in compliance with the principle of gender balance, by decree of the Minister of Economy and Finance, after consulting the Governor of the Bank of Italy, and serve a three-year term, renewable for another three years. Membership on the Committee is not remunerated. The Committee is convened by the Director of the UIF at least every six months and performs advisory and support functions in support of the UIF's work. The Committee also prepares an opinion on the UIF's work, which forms an integral part of the documentation submitted to Parliament pursuant to paragraph 8.

4. The UIF exercises the following functions:

a) receives reports of suspicious transactions and carries out financial analysis thereof; *b)*

analyses financial flows in order to identify and prevent money laundering and terrorist financing phenomena;

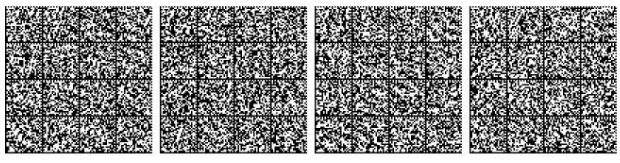
c) may suspend suspicious transactions for a maximum of five business days, including at the request of the Special Currency Unit of the Guardia di Finanza, the Anti-Mafia Investigation Directorate, the judicial authority, or at the request of another FIU, provided this does not prejudice the course of the investigation. The FIU shall immediately notify the requesting authority of the suspension; *d)* taking into account the characteristics of the obligated entities, issues instructions, published in the *Official Journal* of

the Italian Republic, regarding the data and information that must be included in suspicious transaction reports and objective communications, the related timeframes, and the methods for protecting the confidentiality of the reporting party's identity;

e) in order to facilitate the identification of suspicious transactions, issues and periodically updates, after presentation to the Financial Security Committee, anomaly indicators, published in the *Official Journal* of the Italian Republic and in a dedicated section of its institutional website; *f)* carries out checks, including

through inspections, to ensure compliance with the provisions on the prevention and fight against money laundering and terrorist financing, with regard to reports of suspicious transactions and cases of failure to report suspicious transactions, as well as with regard to the communications to the FIU required by this decree and cases of failure to report such transactions, also with the collaboration of the Special Currency Police Unit of the Guardia di Finanza; *g)* in relation to its duties, ascertains and contests or reports to the relevant supervisory authorities any violations of the obligations set forth in this decree of which it becomes aware

in the exercise of its institutional functions;



h) ensures the timely transmission of data, information, and analyses to the National Anti-Mafia and Anti-Terrorism Directorate, as established in Article 8, paragraph 1, letter *a)* . It also ensures that the analyses requested by the National Anti-Mafia and Anti-Terrorism Directorate are carried out pursuant to Article 8, paragraph 1, letter *d)* .

5. In order to carry out its institutional functions, the UIF: *a)* acquires, including through inspections, data and information at the subjects to whom the obligations set forth in this decree are addressed;

b) receives the communication of aggregate statistical data from the entities required to do so and the communications to which the Public Administrations are required to provide, pursuant to Article 10.

6. To exercise the functions referred to in paragraphs 4 and 5, the UIF:

a) uses the data contained in the register of accounts and deposits referred to in Article 20, paragraph 4, of Law No. 413 of 30 December 1991, and in the tax register referred to in Article 37 of Legislative Decree No. 223 of 4 July 2006, converted, with amendments, by Law No. 248 of 4 August 2006;

b) has access to the data and information contained in the integrated real estate register referred to in Article 19 of Legislative Decree No. 78 of 31 May 2010, converted, with amendments, by Law No. 122 of 30 July 2010;

c) has access to information on the beneficial owner of legal entities and express trusts, contained in a specific section of the Company Register, pursuant to Article 21 of this decree.

7. Using the information collected in the performance of its functions, the UIF:

a) conducts analyses and studies on individual anomalies, relating to hypotheses of money laundering and terrorist financing in specific sectors of the economy deemed at risk, in categories of payment instruments, and in specific territorial economic situations, also based on the national risk analysis developed by the Financial Security Committee; *b)* develops and disseminates models and diagrams representing anomalous economic and financial behaviors attributable to possible money laundering and terrorist financing activities.

8. For the purposes of submitting to Parliament the report on the status of the action to prevent money laundering and terrorist financing, the Director of the UIF, by 30 May of each year, shall transmit to the Minister of Economy and Finance, through the Financial Security Committee, the annexes to the same report, referred to in Article 4, paragraph 2, of this decree.».

— The text of Articles 4, 6, 7, and 43 of Law No. 124 of August 3, 2007 (Information System for the Security of the Republic and New Secrecy Regulations), published in the Official Journal of August 13, 2007, No. 187, is reported below:

«Art. 4 *(Department of Security Information)* .

1. To carry out the tasks referred to in paragraph 3, the Department of Security Information (DIS) is established within the Presidency of the Council of Ministers.

2. The President of the Council of Ministers and the Delegated Authority, where established, shall avail themselves of the DIS to exercise their powers, in order to ensure full unity in the planning of intelligence research by the Security Information System, as well as in the analyses and operational activities of the security intelligence services.

3. The DIS carries out the following tasks:

a) coordinates all security intelligence activities, also verifying the results of the activities carried out by the AISE and the AISI, without prejudice to the competence of the aforementioned services with respect to intelligence-gathering activities and collaboration with the security services of foreign states;

b) is constantly informed of the operations under the jurisdiction of the security intelligence services and transmits them to the President of the Council of Ministers the information and analyses produced by the Security Information System;

c) collects information, analyses, and reports from security intelligence services, the Armed Forces and the police, state administrations, and research institutions, including private ones; without prejudice to the exclusive competence of the AISE and AISI for the development of their respective operational research plans, it develops strategic analyses or analyses relating to specific situations; formulates assessments and forecasts, based on the sectoral analytical contributions of the AISE and AISI;

d) prepares, also on the basis of the information and reports referred to in letter *c)* , global analyses to be submitted to the CISR, as well as pro-information research projects, on which the President of the Council of Ministers decides, after having acquired the opinion of the CISR; d *-bis)* on the basis of the directives referred to in Article 1, paragraph 3 - *bis* as well as the information and reports referred to in letter *c)* of this paragraph, coordinates information-gathering activities aimed at strengthening national cyber protection and information security; *e)* promotes and guarantees, including through periodic meetings, the exchange of information between the AISE, the AISI and the police forces; communicates to the President of the Council of Ministers the findings resulting from the exchange of information and the results of the periodic meetings;

f) transmits, upon order of the President of the Council of Ministers, after consulting the CISR, information and analyses to public administrations or entities, including autonomous entities, interested in acquiring security information; *g)* develops, in agreement with the AISE and the AISI, the plan for the acquisition of human and material resources and any other resources instrumental to the activity of the security intelligence services, to be submitted to the President of the Council of Ministers for approval;

h) after consulting AISE and AISI, prepares and submits for approval by the President of the Council of Ministers the draft regulation referred to in Article 21, paragraph 1;

(i) exercises oversight over the AISE and AISI, verifying the compliance of security intelligence activities with laws and regulations, as well as with the directives and provisions of the President of the Council of Ministers. For this purpose, an inspection office is established within the DIS, whose organizational and operational procedures are defined in the regulation referred to in paragraph 7. The annual activity plan of the inspection office is approved annually in accordance with the procedures set forth in this regulation, subject to the opinion of the Parliamentary Committee referred to in Article 30. The inspection office, within the scope of the responsibilities defined in the aforementioned regulation, may conduct internal investigations into specific incidents and behaviors occurring within the security intelligence services, including at the request of the Director General of the DIS, authorized by the President of the Council of Ministers;

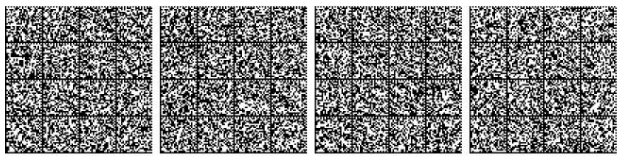
l) ensures the implementation of the provisions issued by the President of the Council of Ministers with a specific regulation adopted pursuant to Article 1, paragraph 2, for the purposes of the administrative protection of state secrets and secrecy classifications, also supervising their correct application; *m)* ensures the promotion and dissemination of the culture of security and institutional communication; *n)* provides guidelines for the unified management of the personnel referred to in Article 21, according to the methods defined by the regulation referred to in paragraph 1 of the same article; n *-bis)* manages joint procurement and logistics services on a unitary basis, without prejudice to the operational competences of the AISE and the AISI.

4. Without prejudice to the provisions of Article 118 *-bis* of the Code of Criminal Procedure, introduced by Article 14 of this law, if the information requested from the police forces, pursuant to letters *c)* and *e)* of paragraph 3 of this article, relates to judicial police investigations, such information, if covered by the confidentiality referred to in Article 329 of the Code of Criminal Procedure, may be acquired only with the prior authorization of the competent judicial authority. The judicial authority may also transmit the documents and information on its own initiative.

5. The general management of the DIS is entrusted to a first-level manager or equivalent in the State administration, whose appointment and dismissal are the sole responsibility of the President of the Council of Ministers, after consulting the CISR. The appointment has a maximum term of eight years and may be conferred, without interruption, even by subsequent measures, each of which lasts no longer than four years.

Pursuant to this law, the Director of the DIS is the direct report of the President of the Council of Ministers and of the Delegated Authority, where established, except as provided for in Article 6, paragraph 5, and Article 7, paragraph 5, and is hierarchically and functionally superior to the staff of the DIS and of the offices established within the same Department.

6. The President of the Council of Ministers, after consulting the Director General of the DIS, appoints one or more Deputy Directors General; the Director General assigns other duties within the Department, with the exception of those assigned by the President of the Council of Ministers.



7. The organization of the DIS and the offices established within the same Department are governed by specific regulations.

8. The regulation provided for in paragraph 7 defines the organizational and operating methods of the inspection office referred to in paragraph 3, letter *i)* , according to the following criteria:

a) inspectors are guaranteed full autonomy and independence of judgment in the exercise of their control functions; *b)* unless specifically

authorized by the President of the Council of Ministers or the Delegated Authority, where established, controls must not interfere with ongoing operations;

c) specific selection tests and adequate training are foreseen for inspectors; *d)* the transfer of personnel

from the inspection office to the security intelligence services is not permitted;

e) the inspectors, subject to authorization from the President of the Council of Ministers or the delegated Authority, where established, may access all documents held by the security intelligence services and the DIS; they may also acquire, through the Director General of the DIS, other information from public and private bodies. — 1. The *Agency for External Information and Security* (AISE) is established, which

is entrusted with the task of researching and processing, within its areas of competence, all information useful for defending the independence, integrity and security of the Republic, also in implementation of international agreements, from threats from abroad.

2. AISE is also responsible for counter-proliferation activities concerning strategic materials, as well as security information activities, which take place outside national territory, to protect Italy's political, military, economic, scientific and industrial interests.

3. It is also the task of the AISE to identify and counter espionage activities directed against Italy and activities aimed at damaging national interests outside national territory.

4. AISE may conduct operations within the national territory only in collaboration with AISI, when such operations are closely related to activities that AISE itself conducts abroad. To this end, the Director General of DIS shall ensure the necessary coordination and information sharing, also to avoid functional or territorial overlaps.

5. AISE answers to the President of the Council of Ministers.

6. The AISE shall promptly and continuously inform the Minister of Defense, the Minister of Foreign Affairs, and the Minister of the Interior regarding matters falling within their respective areas of competence.

7. The President of the Council of Ministers, by decree, appoints and dismisses the director of the AISE, chosen from among first-level or equivalent managers of the State administration, after consulting the CISR.
The appointment has a maximum duration of eight years and can be conferred, without interruption, even with subsequent provisions, each of which lasts no longer than four years.

8. The Director of the AISE reports regularly on its activities to the President of the Council of Ministers or to the Delegated Authority, where established, through the Director General of the DIS. He reports directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances require it, promptly informing the Director General of the DIS. He submits an annual report on the Agency's functioning and organization to the CISR, through the Director General of the DIS.

9. The President of the Council of Ministers, after consulting the Director of AISE, appoints and dismisses one or more Deputy Directors. The Director of AISE assigns other roles within the Agency.

10. The organization and functioning of the AISE are governed by a specific regulation. — 1. The Agency for Information

and Internal Security (AISI) is established.

"Art. 7 *(Information and Internal Security Agency)* . - The Agency for Information and Internal Security (AISI) is entrusted with the task of researching and processing, within its areas of competence, all information useful for defending, including in implementation of international agreements, the internal security of the Republic and the democratic institutions established by the Constitution at its foundation from any threat, any subversive activity and any form of criminal or terrorist aggression.

2. The AISI is responsible for security intelligence activities carried out within the national territory to protect Italy's political, military, economic, scientific, and industrial interests. 3. The AISI is also responsible for identifying and countering espionage

activities within the national territory directed against Italy and activities aimed at harming national interests.

4. AISI may carry out operations abroad only in collaboration with AISE, when such operations are strictly connected to activities that AISI itself carries out within the national territory.
To this end, the Director General of the DIS ensures the necessary forms of coordination and information sharing, also with the aim of avoiding functional or territorial overlaps.

5. The AISI answers to the President of the Council of Ministers.

6. The AISI shall promptly and continuously inform the Minister of the Interior, the Minister of Foreign Affairs, and the Minister of Defense regarding matters falling within their respective areas of competence.

7. The Prime Minister appoints and dismisses, by decree, the Director of the AISI, selected from among the first-tier or equivalent managers of the State administration, after consulting the CISR. The appointment has a maximum term of eight years and may be conferred, without interruption, even by subsequent measures, each of which lasts no longer than four years.

8. The Director of the AISI reports regularly on its activities to the President of the Council of Ministers or to the Delegated Authority, where established, through the Director General of the DIS. He reports directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances require it, promptly informing the Director General of the DIS. He submits an annual report on the functioning and organization of the Agency to the CISR, through the Director General of the DIS.

9. The President of the Council of Ministers, after consulting the Director of the AISI, appoints and dismisses one or more Deputy Directors. The Director of the AISI assigns other roles within the Agency.

10. The organization and functioning of the AISI are governed by specific regulations.

«Art. 43 *(Procedure for the adoption of regulations)* . — 1. Unless otherwise established, the regulatory provisions set forth in this law shall be issued within one hundred and eighty days of its entry into force, with one or more decrees of the President of the Council of Ministers adopted also in derogation from Article 17 of Law No. 400 of 23 August 1988, and subsequent amendments, following the opinion of the Parliamentary Committee referred to in Article 30 and having consulted the CISR.

2. The aforementioned decrees establish the regime of their publicity, even in derogation from the current regulations.».

— The Treaty on the Functioning of the European Union (version (current) is published in the Official Journal of the European Union of 26 October 2012 no. 326 series C.

Notes to Article 6:

— For references to Commission Recommendation No. 361 of 6 May 2003, see the notes to Article 3.

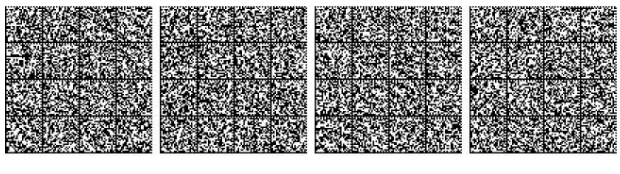
«Art. 2 *(Effective and financial thresholds defining the categories of companies)* . — 1. The category of micro, small and medium-sized enterprises (SMEs) consists of enterprises which employ fewer than 250 persons and whose annual turnover does not exceed EUR 50 million or whose annual balance sheet total does not exceed EUR 43 million.

2. In the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and has an annual turnover or annual balance sheet total not exceeding 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.».

Notes to Article 8:

— The text of Legislative Decree No. 196 of June 30, 2003, containing the "Personal Data Protection Code, containing provisions for the adaptation of national legislation to Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" is published in the *Official Journal* of July 29, 2003, No. 174, SO.



— For references to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2022 (Directive on privacy and electronic communications), see the notes to the introduction.

Notes to Article 9:

— For references to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, see the notes to the preamble.

— The text of Article 2 of the aforementioned Legislative Decree of 14 June 2021, no. 82, is reported below.

«Art. 2 *(Powers of the President of the Council of Ministers)* .

— 1. The following powers are attributed exclusively to the President of the Council of Ministers:

a) the senior management and overall responsibility for cybersecurity policies; *b)* the adoption of the

national cybersecurity strategy, after consulting the Interministerial Committee for Cybersecurity (CIC) referred to in Article 4; *c)* the appointment and dismissal of the Director General

and Deputy Director General of the National Cybersecurity Agency referred to in Article 5, following a resolution of the Council of Ministers.

2. For the purposes of exercising the powers referred to in paragraph 1, letter *a)* , and the implementation of the national cybersecurity strategy, the President of the Council of Ministers, after consulting the CIC, issues cybersecurity directives and all provisions necessary for the organization and functioning of the National Cybersecurity Agency.

3. The President of the Council of Ministers shall inform in advance the Parliamentary Committee for the Security of the Republic (CO-PASIR), referred to in Article 30 of Law No. 124 of 3 August 2007, and the competent Parliamentary Commissions of the appointments referred to in paragraph 1, letter *c)* , of this Article.

— The text of Article 7 of the aforementioned Legislative Decree of 14 June 2021, no. 82, is reported

below: «Art. 7 *(Functions of the National Cybersecurity Agency)* .

— 1. The Agency:

a) is the National Authority for Cybersecurity and, in relation to this role, ensures, in compliance with the responsibilities attributed by current legislation to other administrations, without prejudice to the powers of the Minister of the Interior as national public security authority, pursuant to Law no. 121 of 1 April 1981, coordination between public bodies involved in cybersecurity matters at the national level and promotes the implementation of joint actions aimed at ensuring cybersecurity and resilience for the development of the digitalization of the country, the production system and public administrations, as well as for the achievement of national and European autonomy with regard to IT products and processes of strategic importance for the protection of national interests in the sector. For networks, information systems and IT services relating to the management of classified information, the provisions of the regulation adopted pursuant to Article 4, paragraph 3, letter *l)* , of Law no. 124 of 2007, as well as the powers of the Central Office for Secrecy referred to in Article 9 of the same Law no. 124 of 2007; *b)* prepares the national cybersecurity strategy; *c)* carries out all necessary support activities for the functioning of the Cybersecurity Unit, referred to in Article 8; *d)* is the competent national authority and single point of contact for matters of network and information systems security, for the purposes set out in the

NIS Legislative Decree, to protect the legal unity of the legal system,

and is responsible for ascertaining violations and imposing the administrative sanctions provided for by the same decree;

e) is the National Cybersecurity Certification Authority pursuant to Article 58 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, and assumes all the cybersecurity certification functions already attributed to the Ministry of Economic Development by current legislation, including those relating to the identification of violations and the imposition of sanctions; in carrying out the tasks referred to in this letter:

1) accredits, pursuant to Article 60, paragraph 1, of Regulation (EU) 2019/881 of the European Parliament and of the Council, the specialized structures of the Ministry of Defence and the Ministry of the Interior as conformity assessment bodies for the systems under their respective competence;

2) delegates, pursuant to Article 56, paragraph 6, letter *b)* , of Regulation (EU) 2019/881 of the European Parliament and of the Council, the Ministry of Defence and the Ministry of the Interior, through their respective accredited structures referred to in point 1) of this letter, to issue the European cybersecurity certificate;

f) assumes all cybersecurity functions already assigned to the Ministry of Economic Development by current provisions, including those relating to: 1) the perimeter of national cybersecurity, pursuant to the

Perimeter Decree-Law and its implementing provisions, including the functions assigned to the National Evaluation and Certification Center pursuant to the Perimeter Decree-Law, the inspection and verification activities referred to in Article 1, paragraph 6, letter *c)* , of the Perimeter Decree-Law and those relating to the identification of violations and the imposition of administrative sanctions provided for by the same decree, without prejudice to those referred to in Article 3 of the regulation adopted by Decree of the President of the Council of Ministers of 30 July 2020, no. 131; 2) the security and integrity of electronic communications, pursuant to Articles 16 *-bis* and 16 *-ter* of Legislative Decree no. 259 of 1 August 2003, and its

implementing provisions;

3) the security of networks and information systems, pursuant to the NIS Legislative Decree; *g)* participates,

within its areas of competence, in the coordination group established pursuant to the regulations referred to in Article 1, paragraph 8, of Legislative Decree no. 21 of 15 March 2012, converted, with amendments, by Law no. 56 of 11 May 2012; *h)* assumes all the functions attributed to the Presidency of the

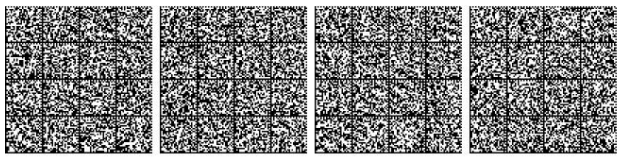
Council of Ministers regarding the perimeter of national cyber security, pursuant to the Perimeter Decree-Law and the related implementing provisions, including the inspection and verification activities referred to in Article 1, paragraph 6, letter *c)* , of the Perimeter Decree-Law and those relating to the identification of violations and the imposition of administrative sanctions provided for by the same decree, without prejudice to those referred to in Article 3 of the regulation adopted by Decree of the President of the Council of Ministers no. 131 of 2020; *i)* assumes all the functions already assigned to the Department of Security Information (DIS), pursuant to Article 4 of Law No. 124 of 3 August 2007, by the Perimeter Decree-Law and

the related implementing provisions, and supports the President of the Council of Ministers for the purposes of Article 1, paragraph 19 *-bis* of the Perimeter Decree-Law; *l)* provides, on the basis of the activities under the jurisdiction of the Cybersecurity Unit referred to in Article 8, the activities necessary for the implementation and monitoring of the execution of the provisions adopted by the President of

the Council of Ministers pursuant to Article 5 of the Perimeter Decree-Law;

m) assumes all cybersecurity functions already assigned to the Agency for Digital Italy under current provisions, and in particular, those referred to in Article 51 of Legislative Decree No. 82 of 7 March 2005, as well as those relating to the adoption of guidelines containing technical cybersecurity rules pursuant to Article 71 of the same Legislative Decree. The Agency also assumes the tasks referred to in Article 33- *septies* , paragraph 4, of Legislative Decree No. 179 of 18 October 2012, converted, with amendments, by Law No. 221 of 17 December 2012, previously assigned to the Agency for Digital Italy; m *-bis)* provides, including through a specific section within the strategy referred to in letter *b)* , for the development and dissemination of

standards, guidelines, and recommendations to strengthen the cybersecurity of information systems, the assessment of the security of cryptographic systems, and the organization and management of dissemination activities aimed at promoting the use of cryptography, including blockchain technology, as a cybersecurity tool. The Agency, also to strengthen Italy's industrial and technological autonomy, promotes collaboration with university and research centers to enhance the development of new proprietary algorithms, research, and the achievement of new national cryptographic capabilities, as well as international collaboration with foreign organizations that perform similar functions. To this end, the National Cryptography Center is established within the Agency, within the human, instrumental, and financial resources available under current legislation and without new or increased burdens on public finances. Its operation is regulated by a provision of the Agency's Director General. The National Cryptography Center serves as a national center of expertise for all aspects of cryptography in unclassified areas, without prejudice to the powers of the Central Office for Secrecy, pursuant to Article 9 of the law.



3 August 2007, no. 124, with reference to the information and activities provided for by the regulation adopted pursuant to Article 4, paragraph 3, letter *l) ,* of the aforementioned Law no. 124 of 2007, as well as the competences of the bodies referred to in Articles 4, 6 and 7 of the same law;

m *-ter)* provides for the qualification of cloud services for public administration in compliance with European Union legislation and the regulation referred to in Article 33 *-septies ,* paragraph 4, of Legislative Decree No. 179 of 18 October 2012, converted, with amendments, by Law No. 221 of 17 December 2012; *n)* develops national prevention, monitoring,

detection, analysis, and response capabilities to prevent and manage cybersecurity incidents and cyber attacks, including through the CSIRT Italy referred to in Article 8 of the NIS Legislative Decree. To this end, it promotes public-private partnership initiatives to make these capabilities effective;

n *-bis)* within the scope of the functions referred to in the first sentence of letter *n) ,* carries out all activities aimed at analyzing and providing support for the containment and restoration of the operation of compromised systems, with the collaboration of public or private entities that have suffered IT security incidents or cyber attacks. The failure to cooperate referred to in the first sentence is assessed for the purposes of applying the sanctions provided for in Article 1, paragraphs 10 and 14, of the Perimeter Decree-Law, for the entities referred to in Article 1, paragraph 2 *-bis of* the Perimeter Decree-Law, referred to in Article 3, paragraph 1, , of the same letters *g)* and *i) ,* of the NIS Legislative Decree and referred to in Article 40, paragraph 3, subparagraph, of the Electronic Communications Code, referred to in Legislative Decree no. 259 of 1 August 2003; excluding the State bodies responsible for the prevention, detection, and repression of crimes, the protection of public order and safety, and the defense and military security of the State, as well as the security intelligence bodies referred to in Articles 4, 6, and 7 of Law No. 124 of August 3, 2007; (n *-ter)* collects, processes, and classifies data relating to incident notifications received from entities required to do so in compliance with current

provisions. Such data shall be made public in the report provided for in Article 14, paragraph 1, as official reference data for cyber attacks carried out on entities operating in sectors relevant to national interests in the field of cybersecurity. The obligations set forth in this letter shall be fulfilled with the human, instrumental, and financial resources available under current legislation; *(o)* participates in national and international exercises involving the simulation of cyber events in order to increase the country's resilience;

p) oversees and promotes the definition and maintenance of an updated and coherent national legal framework in the cybersecurity domain, also taking into account international guidelines and developments. To this end, the Agency expresses non-binding opinions on legislative or regulatory initiatives concerning cybersecurity;

q) coordinates, in conjunction with the Ministry of Foreign Affairs and International Cooperation, international cooperation in the field of cybersecurity. Within the European Union and internationally, the Agency maintains relations with the competent bodies, institutions, and agencies, as well as monitors cybersecurity issues in the relevant institutional forums, except for areas where the law assigns specific responsibilities to other administrations. In such cases, coordination with the Agency is ensured to ensure unified national positions consistent with the cybersecurity policies defined by the Prime Minister;

r) pursuing objectives of excellence, supports the development of industrial, technological, and scientific skills and capabilities within its areas of expertise, through the involvement of the national university and research system as well as the national production system. To these ends, the Agency may promote, develop, and finance specific projects and initiatives, also aimed at fostering the technology transfer of research results in the sector. The Agency ensures the necessary coordination with other administrations to which the law assigns competences in the field of cybersecurity and, in particular, with the Ministry of Defense for aspects related to military research. The Agency may also promote the establishment of areas dedicated to the development of innovation aimed at fostering the training and recruitment of personnel in advanced sectors of cybersecurity development, as well as promoting the implementation of feasibility studies and evaluation analyses aimed at this purpose.

scope;

s) enters into bilateral and multilateral agreements, including through the involvement of the private and industrial sectors, with institutions, bodies, and organizations in other countries for Italy's participation in cybersecurity programs, ensuring the necessary coordination with other administrations to which the law assigns cybersecurity responsibilities, without prejudice to the responsibilities of the Ministry of Foreign Affairs and International Cooperation; *t)* promotes, supports, and coordinates Italy's participation in

European Union and international projects and initiatives, including through the involvement of national public and private entities, in the field of cybersecurity and related application services, without prejudice to the responsibilities of the Ministry of Foreign Affairs and International Cooperation. The Agency ensures the necessary coordination with other administrations to which the law assigns cybersecurity responsibilities, and in particular with the Ministry of Defense for aspects relating to projects and initiatives in collaboration with NATO and the European Defense Agency; *u)* carries out communication and awareness-raising activities in the field of cybersecurity, in order to contribute to the development of a national culture in this area; *v)* promotes training, technical and professional growth,

and the qualification of human resources in the field of cybersecurity, in particular by encouraging the activation of university training programs in the field, including through the awarding of scholarships,

doctorates, and research grants, based on specific agreements with public and private entities; in carrying out these tasks, the Agency may also avail itself of the training facilities and capabilities of the Presidency of the Council of Ministers, the Ministry of Defense, and the Ministry of the Interior, according to terms and methods to be defined by a specific decree of the President of the Council of Ministers, in consultation with the relevant Ministers;

(v *-bis)* may arrange specific training activities reserved for young people participating in the civil service, regulated on the basis of specific agreements. In any case, the service provided is, for all intents and purposes, recognized as civil service; (z) for the purposes set out in this article,

may establish and participate in public-private partnerships throughout the country, as well as, subject to the authorization of the President of the Council of Ministers, in consortia, foundations, or companies with public and private entities, both Italian and foreign;

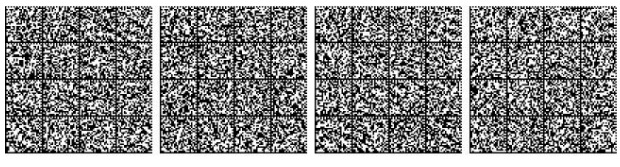
aa) is designated as the National Coordination Centre pursuant to Article 6 of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021, establishing the European Competence Centre for Cybersecurity in the Industrial, Technological and Research Sectors and the Network of National Coordination Centres. 1 *-bis .* Also for the purposes of exercising the functions referred to in paragraph 1, letters *r) , s) , t) , u) , v) , z)* and *aa) ,* a Technical-Scientific Committee is established within the Agency, with advisory and proposal functions, chaired by the Director General of the same Agency, or by a manager delegated by him, and composed of staff of the same Agency and qualified representatives of industry, research institutions, academia and associations in the security sector, designated by decree of the President of the Council of Ministers. The composition and organization of the Technical-Scientific Committee are governed by the methods and criteria defined in the regulation referred to in Article 6, paragraph 1. No attendance fees, compensation or reimbursement of expenses are provided for participation in the Technical-Scientific Committee.

2. Within the Agency, the national representative and his/her deputy shall be appointed, by decree of the President of the Council of Ministers, to the Governing Board of the European Competence Centre for Cybersecurity in the Industrial, Technological and Research sectors, pursuant to Article 12 of Regulation (EU) 2021/887.

3. The Italian CSIRT referred to in Article 8 of the NIS Legislative Decree is transferred to the Agency and takes the name: “CSIRT Italia”.

4. The National Evaluation and Certification Center, established at the Ministry of Economic Development, is transferred to the Agency.

5. In accordance with the powers of the Italian Data Protection Authority, the Agency, for the purposes set out in this decree, consults and collaborates with the Authority, including in relation to incidents involving personal data breaches. The Agency and the Authority may enter into specific memoranda of understanding that also define the modalities of their collaboration within the available resources.



in accordance with current legislation and without new or increased burdens on public finances.».

Notes to Article 10:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 11:

— The text of Article 30 of Legislative Decree No. 165 of March 30, 2001 (General provisions on the organization of work within public administrations) is reported below: «Art. 30 *(Direct transfer of personnel between different administrations)* .

— 1. Administrations may fill vacant positions through the direct transfer of employees referred to in Article 2, paragraph 2, holding a corresponding qualification and currently employed by other administrations, who apply for transfer. The prior consent of the administration to which the transferor belongs is required if the positions in question have been justified as non-fungible by the transferring administration, if the transfer involves personnel employed less than three years previously, or if the transfer results in a staff shortage of more than 20 percent in the qualification corresponding to that of the applicant. The possibility of deferring, for justified organizational reasons, the direct transfer of the employee for up to sixty days from receipt of the request for direct transfer to another administration remains unaffected. The provisions of the second and third paragraphs do not apply to the personnel of companies and entities of the National Health Service and local authorities with a number of permanent employees not exceeding 100, for which the prior consent of the administration to which the transferor belongs is still required. Current provisions on this matter continue to apply to school staff. Administrations, having established the required professional qualifications and skills in advance, publish a notice on their institutional website for a period of at least thirty days. This notice lists the positions they intend to fill through direct transfers of staff from other administrations, along with the required qualifications. On an experimental basis and until new procedures for determining standard personnel needs in public administrations are introduced, transfers between the headquarters of different ministries, agencies, and national non-economic public bodies do not require the consent of the home administration. The home administration will arrange the transfer within two months of the request from the new administration, subject to notice periods and provided that the new administration has a higher percentage of vacancies than the home administration.

1.1. For local authorities with between 101 and 250 employees, the percentage referred to in paragraph 1 is set at 5 percent; for local authorities with no more than 500 employees, the aforementioned percentage is set at 10 percent. The percentage referred to in paragraph 1 is to be considered following the mobility and is based on the institution's staffing. 1 *-bis* . The receiving administration shall provide retraining for employees whose transfer

requests are accepted, possibly making use of the National School of Administration where necessary, to develop specific or sector-specific training programs.

This paragraph will be implemented using the human, instrumental, and financial resources available under current legislation and, in any case, without new or increased burdens on public finances.

1 *-ter* . An employee who is a victim of gender-based violence and is enrolled in specific protection programs, duly certified by the social services of the municipality of residence, may apply for transfer to another public administration located in a municipality other than that of residence, after notifying the administration to which she belongs. Within fifteen days of the aforementioned notification, the administration to which she belongs will arrange for the transfer to the administration indicated by the employee, if there are vacancies corresponding to her professional qualifications. 1 *-quater* .

Starting from 1 July 2022, for the purposes referred to in paragraph 1 and in any case of initiation of mobility procedures, the administrations shall publish the relevant notice in a specific section of the Single Recruitment Portal referred to in Article 35 *-ter.* Personnel interested in participating in the aforementioned procedures shall send their application, for any available position, after registering on the Portal.

accompanied by their CV, exclusively in digital format. This provision must not result in new or increased burdens on public finances.

1 *-quinquies* . For non-managerial staff of the administrations referred to in Article 1, paragraph 2, of the independent administrative authorities, and of the entities referred to in Article 70, paragraph 4, secondments or secondments are permitted exclusively within the limit of 25 percent of the positions not filled following the mobility procedures referred to in this Article. The provision set forth in the first sentence does not apply to mandatory secondments or secondments required by law, including those relating to direct collaboration offices, nor to those relating to participation in bodies, however named, established by legislative or regulatory provisions that provide for the participation of staff from different administrations, nor to secondments to the territorial offices of ministries, or to the Unions of Municipalities for the municipalities that are part of them.

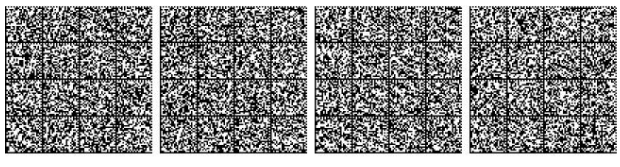
2. Within the scope of the employment relationships referred to in Article 2, paragraph 2, employees may be transferred within the same administration or, by agreement between the administrations involved, to another administration, to offices located within the same municipality or no more than fifty kilometers from their current location. For the purposes of this paragraph, the third sentence of the first paragraph of Article 2103 of the Civil Code does not apply. By decree of the Minister for Simplification and Public Administration, after consultation with the representative trade union confederations and, where necessary, after consultation with the unified conference referred to in Article 8 of Legislative Decree No. 281 of 28 August 1997, criteria may be established for implementing the processes referred to in this paragraph, including direct transfers of personnel between administrations without prior agreement, to ensure the performance of institutional functions by administrations experiencing staff shortages. The provisions of this paragraph apply to employees with children under the age of three, who are entitled to parental leave, and to the persons referred to in Article 33, paragraph 3, of Law No. 104 of 5 February 1992, and subsequent amendments, with their consent to perform their work activities elsewhere.

2.1. In the cases referred to in paragraphs 1 and 2 for which a transfer of resources is necessary, paragraph 2.3 shall apply.

2.2 National collective agreements may integrate the general procedures and criteria for the implementation of the provisions of paragraphs 1 and 2. Any agreements, deeds or clauses of collective agreements that conflict with the provisions of paragraphs 1 and 2 are null and void.

2.3 In order to facilitate the processes referred to in paragraphs 1 and 2, a fund for improving staff allocation within public administrations is established in the budget of the Ministry of Economy and Finance. The fund is allocated €15 million for 2014 and €30 million starting in 2015, to be allocated to the administrations receiving the aforementioned processes. The fund will also receive resources corresponding to fifty percent of the remuneration due to transferred personnel through payment to the State Revenue Agency by the transferring administration and corresponding reallocation to the fund or through a simultaneous reduction in state transfers to the transferring administration. The criteria for using and methods for managing the fund's resources are established by decree of the President of the Council of Ministers, in consultation with the Minister of Economy and Finance. During the initial application phase, the allocation of resources will prioritize requests aimed at ensuring the optimal functioning of judicial offices with significant staff shortages and, consequently, the full implementation of the provincial reform pursuant to Law No. 56 of 7 April 2014. Resources will be allocated to the receiving administrations until the personnel subject to the procedures referred to in paragraphs 1 and 2 are effectively employed.

2.4 The costs arising from the implementation of paragraph 2.3, equal to 15 million euros for the year 2014 and 30 million euros starting from the year 2015, shall be covered, as regards 6 million euros for the year 2014 and 9 million euros starting from 2015, by means of a corresponding reduction in the spending authorization referred to in article 3, paragraph 97, of law no. 244 of 24 December 2007, and as regards 9 million euros starting from 2014, by means of a corresponding reduction in the spending authorization referred to in article 1, paragraph 14, of decree law no. 262 of 3 October 2006 converted with amendments by law no. 24 November 2006. 286 and 12 million euros starting from 2015 through a corresponding reduction in the spending authorization referred to in Article 1, paragraph 527, of Law 27 December 2006, n. 296. Starting from 2015, the fund referred to in paragraph 2.3 may be recalculated



Pursuant to Article 11, paragraph 3, letter *d)* , of Law No. 196 of 31 December 2009, the Minister of Economy and Finance is authorized to issue decrees to implement this Article as necessary. 2 *-bis* . Before conducting competitive procedures to fill vacant positions, administrations must activate the mobility

procedures referred to in paragraph 1, providing, as a priority, for the permanent appointment of employees from other administrations, in secondment or non-permanent positions, belonging to the same functional area, who apply for transfer to the roles of the administrations in which they serve. The transfer is arranged, within the limits of vacant positions, with classification in the functional area and economic position corresponding to that held in the administrations of origin; the transfer may also be arranged if the vacancy exists in an area other than that of classification, ensuring the necessary financial neutrality. limitedly

2 *-ter* .The appointment to a permanent position referred to in , paragraph 2 *-bis* at the Presidency of the Council of Ministers and the Ministry of Foreign Affairs, based on the specific professionalism required of their employees, takes place following a comparative evaluation of the service and educational qualifications held by the seconded or non-permanent employees at the time of submitting the transfer request, within the limits of the positions actually available. 2 *-quater* .

In order to address current emergency situations, the Presidency of the Council of Ministers, by virtue of the specific professionalism required of its employees, may reserve positions for personnel hired by ordinance for the needs of Civil Protection and the civil service, within the scope of the competitive procedures referred to in Article 3, paragraph 59, of Law No. 350 of 24 December 2003, and Article 1, paragraph 95, of Law No. 311 of 30 December 2004.

2 *-quinquies* . Unless otherwise provided, following registration in the register of the destination administration, the employee transferred due to mobility shall be subject exclusively to the legal and economic treatment, including additional benefits, provided for in the collective agreements in force in the sector of that administration.

2 *-sexies* Public administrations, for justified organizational needs resulting from the planning documents provided for in Article 6, may use personnel from other administrations on temporary assignment, in accordance with the procedures established by their respective regulations, for a period not exceeding three years, without prejudice to the provisions of specific provisions on the matter, as well as any spending regime provided for by such provisions and by this decree.

— The text of Article 17, paragraph 14, of Law No. 127 of May 15, 1997 (Urgent measures to streamline administrative activity and decision-making and control procedures) is reported below:

«Art. 17 *(Further provisions regarding the simplification of administrative activity and the streamlining of decision-making and control procedures)* .

— *Omitted* . 14. In the event that legal or regulatory provisions require the use of a contingent of personnel in a secondment or secondment position within public administrations, the administrations to which they belong are required to adopt the secondment or secondment provision within fifteen days of the request. *Omitted* .

Notes to Article 13:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the notes to the preamble. — For references to the aforementioned Legislative Decree no. 82 of 14 June 2021,

see the notes to Article 1.

Notes to Article 14:

— The text of Article 7 *-bis* of Legislative Decree No. 144 of 27 July 2005 (Urgent measures to combat international terrorism) is reported, published in the *Official Journal* No. 173 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005, published in the *Official Journal* No. 177 of 1 August 2005.

«Art. 7 *-bis (Telematics security)* . — 1. Without prejudice to the powers of the Information and Security Services, pursuant to Articles 4 and 6 of Law No. 801 of 24 October 1977, the body of the Ministry of the Interior for the security and regularity of telecommunications services

It ensures the IT protection services of critical information infrastructures of national interest identified by decree of the Minister of the Interior, operating through telematic connections defined by specific agreements with the managers of the structures involved.

2. For the purposes referred to in paragraph 1 and for the prevention and repression of terrorist activities or the facilitation of terrorism conducted using information technology, the judicial police officers belonging to the body referred to in paragraph 1 may carry out the activities referred to in Article 4, paragraphs 1 and 2, of Legislative Decree No. 374 of 18 October 2001, converted, with amendments, by Law No. 438 of 15 December 2001, and those referred to in Article 226 of the implementing, coordination and transitional provisions of the Code of Criminal Procedure, referred to in Legislative Decree No. 271 of 28 July 1989, also upon request or in collaboration with the judicial police bodies indicated therein.».

— Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) is published in the Official Journal of the European Union of 4 May 2016, No. 119, Series L.

— Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 is published in the Official Journal of the European Union of 9 April 2008, No 97, Series L.

— Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation, establishing a European Union Aviation Safety Agency, amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 is published in the OJEU of 22 August 2018 No 212 series L.

— Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC is published in the Official Journal of the European Union of 28 August 2014, No 257, Series L.

— For Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (recast), see the notes to the preamble.

— For references to Article 7, paragraph 5, of the aforementioned Legislative Decree no. 82 of June 14, 2021, see the notes to Article 9.

— For Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, see the notes to the preamble.

— For Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, see the notes to the preamble.

Notes to Article 15:

— For references to Article 7, paragraph 1, letter *s)* , of the Legislative Decree June 14, 2021, no. 82, see the notes to Article 9.

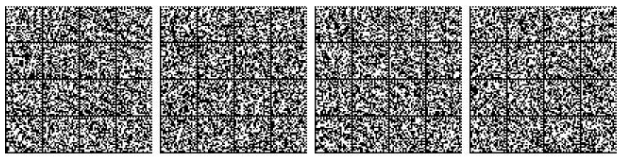
Notes to Article 16:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 17:

— The text of Articles 4, 6 and 7 of Law No. 124 of 2007 (Information System for the Security of the Republic and New Secrecy Regulations), published in the *Official Journal* of 13 August 2007, No. 187, is reported below: «Art. 4 *(Department of Information for Security)* .

1. To carry out the tasks referred to in paragraph 3, the Department of Security Information (DIS) is established within the Presidency of the Council of Ministers.



2. The President of the Council of Ministers and the Delegated Authority, where established, shall avail themselves of the DIS to exercise their powers, in order to ensure full unity in the planning of intelligence research by the Security Information System, as well as in the analyses and operational activities of the security intelligence services.

3. The DIS carries out the following tasks:

a) coordinates all security intelligence activities, also verifying the results of the activities carried out by the AISE and the AISI, without prejudice to the competence of the aforementioned services with respect to intelligence-gathering activities and collaboration with the security services of foreign states;

b) is constantly informed of the operations under the jurisdiction of the security intelligence services and transmits them to the President of the Council of Ministers the information and analyses produced by the Security Information System;

c) collects information, analyses, and reports from security intelligence services, the Armed Forces and the police, state administrations, and research institutions, including private ones; without prejudice to the exclusive competence of the AISE and AISI for the development of their respective operational research plans, it develops strategic analyses or analyses relating to specific situations; formulates assessments and forecasts, based on the sectoral analytical contributions of the AISE and AISI;

d) prepares, also on the basis of the information and reports referred to in letter *c)* , global analyses to be submitted to the CISR, as well as information research projects, on which the President of the Council of Ministers decides, after having acquired the opinion of the CISR; d *-bis)* on the basis of the directives referred to in Article 1, paragraph 3 - *bis* as well as the information and reports referred to in letter *c)* of this paragraph, coordinates information-gathering activities aimed at strengthening national cyber protection and information security; *e)* promotes and guarantees, including through periodic meetings, the exchange of information between the AISE, the AISI and the police forces; communicates to the President of the Council of Ministers the findings resulting from the exchange of information and the results of the periodic meetings;

f) transmits, upon order of the President of the Council of Ministers, after consulting the CISR, information and analyses to public administrations or entities, including autonomous entities, interested in acquiring security information; *g)* develops, in agreement with the AISE and the AISI, the plan for the acquisition of human and material resources and any other resources instrumental to the activity of the security intelligence services, to be submitted to the President of the Council of Ministers for approval; *h)* after consulting the AISE and the AISI, develops and submits to the President of the Council of Ministers for approval the draft regulation referred to in Article 21, paragraph 1;

(i) exercises oversight over the AISE and AISI, verifying the compliance of security intelligence activities with laws and regulations, as well as with the directives and provisions of the President of the Council of Ministers. For this purpose, an inspection office is established within the DIS, whose organizational and operational procedures are defined in the regulation referred to in paragraph 7. The annual activity plan of the inspection office is approved annually in accordance with the procedures set forth in this regulation, subject to the opinion of the Parliamentary Committee referred to in Article 30. The inspection office, within the scope of the responsibilities defined in the aforementioned regulation, may conduct internal investigations into specific incidents and behaviors occurring within the security intelligence services, including at the request of the Director General of the DIS, authorized by the President of the Council of Ministers;

l) ensures the implementation of the provisions issued by the President of the Council of Ministers with a specific regulation adopted pursuant to Article 1, paragraph 2, for the purposes of the administrative protection of state secrets and secrecy classifications, also supervising their correct application; *m)* ensures the promotion and dissemination of the culture of security and institutional communication; *n)* provides guidelines for the unified management of the personnel referred to in Article 21, according to the methods defined by the regulation referred to in paragraph 1 of the same article; n *-bis)* manages joint procurement and logistics services on a unitary basis, without prejudice to the operational competences of the AISE and the AISI.

4. Without prejudice to the provisions of Article 118 *-bis* of the Code of Criminal Procedure, introduced by Article 14 of this By law, if the information requested from the police force, pursuant to letters *c)* and *e)* of paragraph 3 of this article, relates to judicial police investigations, such information, if covered by the confidentiality requirement under Article 329 of the Code of Criminal Procedure, may be acquired only with the prior authorization of the competent judicial authority. The judicial authority may also transmit the documents and information on its own initiative.

5. The general management of the DIS is entrusted to a first-level manager or equivalent in the State administration, whose appointment and dismissal are the sole responsibility of the President of the Council of Ministers, after consulting the CISR. The appointment has a maximum term of eight years and may be conferred, without interruption, even by subsequent measures, each of which lasts no longer than four years.
Pursuant to this law, the Director of the DIS is the direct report of the President of the Council of Ministers and of the Delegated Authority, where established, except as provided for in Article 6, paragraph 5, and Article 7, paragraph 5, and is hierarchically and functionally superior to the staff of the DIS and of the offices established within the same Department.

6. The President of the Council of Ministers, after consulting the Director General of the DIS, appoints one or more Deputy Directors General; the Director General assigns other duties within the Department, with the exception of those assigned by the President of the Council of Ministers.

7. The organization of the DIS and the offices established within the same Department are governed by specific regulations.

8. The regulation provided for in paragraph 7 defines the organizational and operational procedures of the inspection office referred to in paragraph 3, letter *i)* , according to the following criteria: *a)* inspectors are guaranteed full autonomy and independence of judgment in the exercise of their control functions; *b)* unless specifically authorized by the President of the Council of Ministers or the Delegated Authority, where established, the controls must not interfere with ongoing operations; *c)* specific selective tests and adequate training are provided for the inspectors; *d)* the transfer of personnel from the inspection office to the security intelligence services is not permitted;

e) the inspectors, subject to authorization from the President of the Council of Ministers or the delegated Authority, where established, may access all documents held by the security intelligence services and the DIS; they may also acquire, through the Director General of the DIS, other information from public and private bodies. » — 1. «Article 6 *(External Information and Security Agency)* . the External Information and Security Agency (AISE) is established, which is entrusted with the task of researching and processing, within its areas of competence, all information useful for defending the independence, integrity and security of the Republic, also in implementation of international agreements, from threats from abroad.

2. AISE is also responsible for counterproliferation activities involving strategic materials, as well as security information activities carried out outside national territory, to protect Italy's political, military, economic, scientific, and industrial interests.

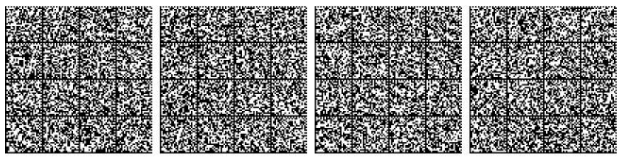
3. It is also the task of the AISE to identify and counter espionage activities directed against Italy and activities aimed at damaging national interests outside national territory.

4. AISE may conduct operations within the national territory only in collaboration with AISI, when such operations are closely related to activities that AISE itself conducts abroad. To this end, the Director General of DIS shall ensure the necessary coordination and information sharing, also to avoid functional or territorial overlaps.

5. AISE answers to the President of the Council of Ministers.

6. The AISE shall promptly and continuously inform the Minister of Defense, the Minister of Foreign Affairs, and the Minister of the Interior regarding matters falling within their respective areas of competence.

7. The President of the Council of Ministers, by decree, appoints and dismisses the director of the AISE, chosen from among first-level or equivalent managers of the State administration, after consulting the CISR.
The appointment has a maximum duration of eight years and can be conferred, without interruption, even with subsequent provisions, each of which lasts no longer than four years.



8. The Director of the AISE reports regularly on its activities to the President of the Council of Ministers or to the Delegated Authority, where established, through the Director General of the DIS. He reports directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances require it, promptly informing the Director General of the DIS. He submits an annual report on the Agency's functioning and organization to the CISR, through the Director General of the DIS.

9. The President of the Council of Ministers, after consulting the Director of AISE, appoints and dismisses one or more Deputy Directors. The Director of AISE assigns other roles within the Agency.

10. The organization and functioning of the AISE are governed by specific regulations.».

Article 7 (Information and Internal Security Agency). — 1. The Information and Internal Security Agency (AISI) is hereby established, entrusted with the task of researching and processing, within its areas of competence, all information useful for defending, including in implementation of international agreements, the internal security of the Republic and the democratic institutions established by the Constitution at its foundation from any threat, any subversive activity, and any form of criminal or terrorist aggression.

2. The AISI is responsible for security intelligence activities carried out within the national territory to protect Italy's political, military, economic, scientific, and industrial interests. 3. The AISI is also responsible for identifying and countering espionage

activities within the national territory directed against Italy and activities aimed at harming national interests.

4. AISI may carry out operations abroad only in collaboration with AISE, when such operations are strictly connected to activities that AISI itself carries out within the national territory.
To this end, the Director General of the DIS ensures the necessary forms of coordination and information sharing, also with the aim of avoiding functional or territorial overlaps.

5. The AISI answers to the President of the Council of Ministers.

6. The AISI shall promptly and continuously inform the Minister of the Interior, the Minister of Foreign Affairs, and the Minister of Defense regarding matters falling within their respective areas of competence.

7. The Prime Minister appoints and dismisses, by decree, the Director of the AISI, selected from among the first-tier or equivalent managers of the State administration, after consulting the CISR. The appointment has a maximum term of eight years and may be conferred, without interruption, even by subsequent measures, each of which lasts no longer than four years.

8. The Director of the AISI reports regularly on its activities to the President of the Council of Ministers or to the Delegated Authority, where established, through the Director General of the DIS. He reports directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances require it, promptly informing the Director General of the DIS. He submits an annual report on the functioning and organization of the Agency to the CISR, through the Director General of the DIS.

9. The President of the Council of Ministers, after consulting the Director of the AISI, appoints and dismisses one or more Deputy Directors. The Director of the AISI assigns other roles within the Agency.

10. The organization and functioning of the AISI are governed by specific regulations.».

Notes to Article 18:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble — For Regulation (EU) No 1025/2012 of the European Parliament

and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/

EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council can be found in the notes to Article 2.

Notes to Article 19:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 20:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 21:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 22:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 25:

— For references to Article 7 *-bis* of Legislative Decree No. 144 of 27 July 2005 (Urgent measures to combat international terrorism) published in the *Official Journal* No. 173 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005, see the notes to Article 14.

Notes to Article 27:

— For Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act'), see the footnotes to the preamble.

Notes to Article 28:

— For Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/
EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council see the notes to Article 2.

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

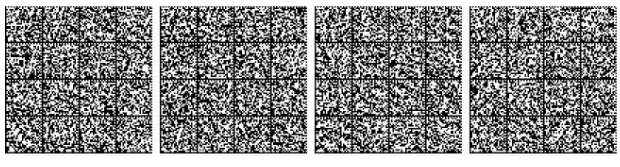
Notes to Article 33:

— The text of Article 1, paragraphs 2 and 2 *-bis* is reported below., of the aforementioned legislative decree no. 105/2019, converted with amendments by law no. 133 of 18 November 2019:

«Art. 1 *(Perimeter of national cyber security)* . — 1.
(Omitted).

2. Within four months from the date of entry into force of the law converting this decree, by decree of the President of the Council of Ministers, adopted on the proposal of the Interministerial Committee for Cybersecurity (CIC): *a)* procedural methods and criteria are

defined for the identification of public administrations, public and private bodies and operators referred to in paragraph 1 having a registered office in the national territory, included in the national cyber security perimeter and required to comply with the measures and



of the obligations set forth in this article; for the purposes of identification, without prejudice to the provisions of Law No. 124 of 3 August 2007 applying to Security Information Bodies, the following criteria shall be used:

1) the subject exercises an essential function of the State, or ensures an essential service for the maintenance of civil, social or economic activities fundamental to the interests of the State; 2) the exercise of such function or the provision of such service uncle depends on networks, information systems and information services;

2 *-bis)* the identification takes place on the basis of a gradual criterion, taking into account the extent of the damage to national security which, in relation to the specificities of the different sectors of activity, may derive from the malfunctioning, interruption, even partial, or improper use of the aforementioned networks, information systems and IT services;

b) the criteria with which the entities referred to in paragraph 2- *bis* prepare and update at least annually a list of the networks, information systems and IT services referred to in paragraph 1, of their respective relevance, including the related architecture and components, are defined on the basis of a risk analysis and a gradual approach that takes into account the specificities of the various sectors of activity. It is understood that, for the networks, information systems and IT services pertaining to the management of classified information, the provisions of the regulation adopted pursuant to Article 4, paragraph 3, letter *l) ,* of Law No. 124 of 3 August 2007 shall apply. The Interministerial Committee referred to in Article 6 of the regulation referred to in Prime Ministerial Decree No. 131 of 30 July 2020 shall develop these criteria by adopting appropriate organizational forms; within six months from the date of the communication, provided for in paragraph 2 *-bis* to each of the entities registered in the list referred to in the same paragraph, the public entities and those referred to in Article 29 of the Digital Administration Code, pursuant to Legislative Decree no. 82 of 7 March 2005, as well as , the private entities, referred to in the aforementioned paragraph 2 *-bis* to the National Cybersecurity Agency, including for the prevention, preparation and management of cyber crises entrusted to the Cybersecurity Unit; the Department of Security Information, the External Information and Security Agency (AISE) and the , transmit such lists Internal Information and Security Agency (AISI) for the purposes of exercising the institutional functions provided for in Articles 1, paragraph 3 *-bis ,* 4, 6 and 7 of Law no. 124 of 2007, as well as the body of the Ministry of the Interior for the security and regularity of telecommunications services referred to in Article 7 *-bis* of Legislative Decree No. 144 of 27 July 2005, converted, with amendments, by Law No. 155 of 31 July 2005, access these lists via the digital platform referred to in Article 9, paragraph 1, of the regulation referred to in Prime Ministerial Decree No. 131 of 2020, established at the National Cybersecurity Agency.

2 *-bis* . The list of entities identified pursuant to paragraph 2, letter *a) ,* is contained in an administrative act, adopted by the President of the Council of Ministers, upon proposal of the CIC, within thirty days of the date of entry into force of the Prime Ministerial Decree referred to in paragraph 2. The aforementioned administrative act, for which the right of access is excluded, is not subject to publication, it being understood that each entity is separately notified without delay of its inclusion in the list. The aforementioned administrative act is updated using the same procedures as those referred to in this paragraph.

2 - *ter* - 19 - *ter* . (Omitted).»

Notes to Article 38:

— For Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, see the notes to the preamble.

— The text of Article 8 *-bis* of Law No. 689 of 24 November 1981 (Amendments to the Penal System), published in the *Official Journal* No. 329 of 30 November 1981, is reported below : «Art. 8 *-bis (Reiteration of Violations) .* — Except as otherwise provided by specific provisions of law, a repeat offense occurs when, within five years of the commission of an administrative violation, ascertained by an enforcement order, the same individual commits another violation of the same nature. A repeat offense also occurs when multiple violations of the same nature committed within the five-year period are ascertained by a single enforcement order.

Violations of the same provision and those of different provisions which, due to the nature of the facts, are considered to be of the same nature which constitute them or by the methods of conduct, present a substantial homogeneity or common fundamental characteristics.

Reiteration is specific if the same provision is violated.

Administrative violations subsequent to the first are not evaluated, for the purposes of repetition, when they are committed in close time and attributable to a single plan.

Reiteration determines the effects that the law expressly provides establishes. It does not apply in the case of reduced payment.

The effects resulting from a repeat offense may be suspended until the provision establishing the previously committed violation becomes final. Suspension is ordered by the competent administrative authority, or, in the event of opposition, by the judge, when serious harm may result.

The effects of the reiteration cease by law, in any case, if the the provision establishing the previous violation is annulled.».

— The text of Article 18 of the aforementioned Legislative Decree of 14 June 2021, no. 82, is reported below: «Art. 18 *(Financial provisions) .* — 1. For the implementation of Articles 5 to 7, a specific chapter is established in the budget estimates of the Ministry of Economy and Finance, with an allocation of 2,000,000 euros for the year 2021, 41,000,000 euros for the year 2022, 70,000,000 euros for the year 2023, 84,000,000 euros for the year 2024, 100,000,000 euros for the year 2025, 110,000,000 euros for the year 2026 and 122,000,000 euros annually starting from the year 2027.

2. The costs referred to in paragraph 1 shall be covered by a corresponding reduction in the Fund referred to in Article 1, paragraph 200, of Law No. 190 of 23 December 2014.

3. The resources entered in the budgets of the administrations concerned, related to the functions redefined pursuant to this decree starting from the start of the operation of the Agency referred to in Article 5, are ascertained, including in residual accounts, by decree of the Minister of Economy and Finance, in agreement with the responsible Ministers, and increased by the Fund referred to in Article 1, paragraph 200, of Law No. 190 of 23 December 2014, also through payment into the State budget and subsequent reallocation to expenditure.

4. The proceeds referred to in Article 11, paragraph 2, shall be paid into the State budget, to be reassigned to the chapter referred to in paragraph 1 of this Article.

5. For the purposes of the immediate implementation of the provisions of this decree, the Minister of Economy and Finance is authorized to make, through his own decrees, including on residual accounts, the necessary budget changes.».

Notes to Article 39:

— For references to Directive (EU) 2022/2555 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 2 Directive), see the footnotes to the preamble.

Notes to Article 40:

— The text of Article 17 of the aforementioned Law of 23 August 1988, no. 400 (Regulation of Government activity and organization of the Presidency of the Council of Ministers) is reported below: «Art. 17 *(Regulations) .* — 1. By decree of the President of the Republic, following a resolution of the Council of Ministers, and having heard the opinion of the Council of State, which must issue a ruling within ninety days of the request, regulations may be issued to regulate:

a) the execution of laws and legislative decrees as well as community regulations; *b)* the implementation and integration of laws and legislative decrees containing principles, excluding those relating to matters reserved to regional jurisdiction;

c) matters in which there is no regulation by laws or by acts having the force of law, provided that these are not matters reserved to the law; *d)* the organisation and functioning of public administrations in accordance with the provisions established by law; *e) .*

2. By decree of the President of the Republic, following a resolution of the Council of Ministers, having heard the Council of State and having received the opinion of the competent parliamentary commissions on the matter, which

they pronounce within thirty days of the request, the regulations are issued for the discipline of the matters not covered by the absolute reserve of law provided for by the Constitution, for which the laws of the Republic, authorizing the exercise of the regulatory power of the Government, determine the general rules governing the matter and provide for the repeal of the existing rules, with effect from the entry into force of the regulatory rules.

3. Regulations may be adopted by ministerial decree in matters within the jurisdiction of the Minister or authorities subordinate to the Minister, when the law expressly grants such power. Such regulations, for matters within the jurisdiction of multiple ministers, may be adopted by interministerial decrees, without prejudice to the requirement for specific authorization by law. Ministerial and interministerial regulations may not establish rules that conflict with those issued by the Government. They must be communicated to the President of the Council of Ministers prior to their promulgation.

4. The regulations referred to in paragraph 1 and the ministerial and inter-ministerial regulations, which must bear the designation "regulation," are adopted after consulting the Council of State, submitted for approval and registration by the Court of Auditors, and published in the *Official Journal* . 4 *-bis* . The organization and discipline of the offices of

the Ministries are determined by regulations issued pursuant to paragraph 2, upon proposal by the competent Minister in agreement with the President of the Council of Ministers and the Minister of the Treasury, in compliance with the principles established by Legislative Decree no. 29 of 3 February 1993, and subsequent amendments, with the contents and observance of the following criteria:

a) reorganization of the offices that directly collaborate with the ministers and Undersecretaries of State, establishing that these offices have exclusive responsibilities in supporting the political management body and liaising between it and the administration;

b) identification of central and peripheral general management-level offices, through diversification between structures with final functions and instrumental functions and their organization by homogeneous functions and according to flexible criteria, eliminating functional duplication; *c)* provision of tools for periodic verification of the organization

and results; *d)* indication and periodic review of the size of the staffing plans; *e)* provision of non-

regulatory ministerial decrees to define the tasks of the management units within the general

management offices. 4 *-ter* . Regulations to be issued pursuant to paragraph 1 of this article shall provide for the periodic reorganization of the regulatory provisions in force, the recognition of those that have

been implicitly repealed, and the express repeal of those that have exhausted their function or are devoid of effective regulatory content or are otherwise obsolete.

— The text of Article 4 of the aforementioned Legislative Decree of 14 June 2021, no. 82, is

reported below: «Art. 4 *(Inter-ministerial Committee for Cybersecurity)* . – 1. The Interministerial Committee for Cybersecurity (CIC) is established at the Presidency of the Council of Ministers, with advisory, proposal and supervisory functions in matters of cybersecurity policies.

2. The Committee:

a) proposes to the President of the Council of Ministers the general guidelines to be pursued within the framework of national cybersecurity policies; *b)* exercises

high surveillance over the implementation of the strategy national cybersecurity;

c) promotes the adoption of necessary initiatives to foster effective collaboration, at the national and international level, between institutional bodies and private operators interested in cybersecurity, as well as for the sharing of information and the adoption of best practices and measures aimed at the objective of cybersecurity and industrial, technological, and scientific development in the field of cybersecurity; *d)* expresses its opinion on the budget and the final budget of the National Cybersecurity Agency.

3. The Committee is chaired by the President of the Council of Ministers and is composed of the Delegated Authority, where established, the Minister of Foreign Affairs and International Cooperation, the Minister of the Interior, the Minister of Justice, the Minister of Defense, the Minister of Economy and Finance, the Minister of Economic Development, the Minister of Ecological Transition, the Minister of Universities and Research, the Minister Delegate for Technological Innovation and the Digital Transition, and the Minister of Sustainable Infrastructure and Mobility.

4. The Director General of the National Cybersecurity Agency nale performs the functions of secretary of the Committee.

5. The President of the Council of Ministers may invite other members of the Council of Ministers, as well as other civil and military authorities whose presence he deems necessary from time to time in relation to the issues to be discussed, to participate in the Committee's meetings, even upon their request, without the right to vote.

6. The Committee also carries out the functions already assigned to the Interministerial Committee for the Security of the Republic (CISR), pursuant to Article 5 of Law No. 124 of 3 August 2007, by the perimeter decree-law and the related implementing provisions, with the exception of those provided for in Article 5 of the same perimeter decree-law.».

Notes to Article 41:

— Legislative Decree No. 65 of 18 May 2018, repealed with effect from 18 October 2024 by this decree, provides: «Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union», and is published in the *Official Journal* No. 132 of 9 June 2018.

— The text of Articles 7, paragraph 8, and 8, paragraph 10, of the aforementioned Legislative Decree of 18 May 2018, no. 65, repealed, effective 1 January 2025 by this decree, is reported below:

«Art. 7 *(National competent authority and single point of contact)* . — 1. – 7. *Omitted* .

8. The costs arising from this article, amounting to 1,300,000 euros per year starting from 2018, shall be covered pursuant to Article 22.»

«Art. 8 *(Incident Response Teams – CSIRT)* . — 1. – 9. *Omitted* .

10. For expenses related to the operation of CSIRT Italy, an annual expenditure of €2,000,000 is authorized starting from 2020. These expenses will be covered pursuant to Article 22.».

— Chapters IV and V of the aforementioned Legislative Decree of 18 May 2018, no. 65, contain, respectively, "Security of the network and information systems of essential service operators" and "Security of the network and information systems of digital service providers".

— The text of Article 2, paragraph 1, letter *h)* , Article 30, paragraph 26, and Articles 40 and 41 of Legislative Decree No. 259 of 1 August 2003 (Electronic Communications Code), published in the *Official Journal* on 15 September 2003, repealed by this provision, is reported below: «Art. 2 *(Definitions)* .

— 1. For the purposes of this decree, it is understood that For:

a) - g) . Omitted .

h) terminal equipment: terminal equipment as defined in Article 1, paragraph 1), of Legislative Decree 26 October 2010 n. 198;

i) – dddd). *Omitted .».*

«Article 30 *(Sanctions)* . — 1.- 25. *Omitted* .

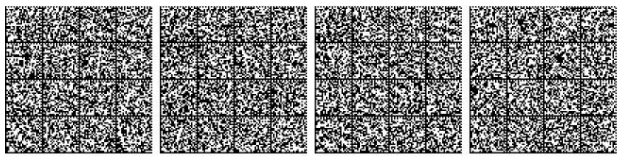
26. Unless the act constitutes a crime, failure to comply with the provisions on information security is punishable by an administrative pecuniary sanction: *a)* from 250,000 to 1,500,000 euros for failure

to comply with the security measures referred to in Article 40, paragraph 3, letter *a) ;*

b) from €300,000 to €1,800,000 for failure to report any significant incident referred to in Article 40, paragraph 3, letter *b) ; c)* from €200,000 to €1,000,000 for failure to

provide the information necessary to assess safety referred to in Article 40, paragraph 3, letter *a)* . 27. – 27- *quinquies* . *Omitted .».*

«Art. 40 (Security of networks and services). — 1. The Agency, after consulting the Ministry, within its respective competence and taking into account the technical and organizational measures that can be adopted by the



The European Commission, pursuant to Article 40, paragraph 5, of Directive (EU) 2018/1972, identifies: *(a)* appropriate

and proportionate technical and organizational measures to manage risks to the security of publicly available electronic communications networks and services, ensuring a level of security appropriate to the risk, taking into account current state of the art. These measures, which may include, where appropriate, the use of encryption techniques, are also intended to prevent and limit the consequences of security incidents for users, interconnected networks, and other services;

b) the cases in which security incidents are to be considered significant for the correct functioning of the networks or services.

2. In determining the cases referred to in paragraph 1, letter *b)* , the Agency considers the following parameters, if available:

(a) the number of users affected by the security incident; *(b)* the duration

of the security incident; *(c)* the geographical

spread of the area affected by the security incident; *(d)* the extent to which the functioning of

the network or service is affected;

e) the extent of the impact on economic and social activities.

3. Undertakings providing public communications networks or publicly accessible electronic communications services:

a) adopt the measures identified by the Agency referred to in paragraph 1, letter *a) ; b)*

communicate to the Agency and to the Computer Security Incident Response Team (CSIRT), established pursuant to Article 8 of Legislative Decree no. 65 of 18 May 2018, any significant security incident as provided for in paragraph 1, letter *b)* .

4. The Agency may inform the public or require the company to do so, where it determines that disclosure of the security incident referred to in paragraph 1(b) is in the public interest. Where appropriate, the Agency shall inform the competent authorities of the other Member States and the European Union Agency for Network and Information Security (ENISA).

5. The Agency, also making use of the CSIRT, shall, directly or through providers of electronic communications networks and services, inform users potentially affected by particular and significant threats of security incidents, regarding any protective measures or remedies they can resort to.

6. The Agency shall annually submit to the European Commission and the European Union Agency for Network and Information Security a summary report of the notifications received and the actions taken in accordance with this Article.

7. In cybersecurity matters, with the exception of areas where the law assigns specific responsibilities to other administrations, the Agency collaborates with the competent authorities of other Member States and with the relevant international and European Union bodies to define procedures and standards that guarantee the security of services.

8. In the event of notification of a security incident that also results in a personal data breach, the Agency shall, without delay, provide the Guarantor for the protection of personal data with the information useful for the purposes referred to in Article 33 of EU Regulation 2016/679 . ».

«Art. 41 *(Implementation and control)* . — 1. The measures adopted for the purposes of implementing this Article and Article 40 shall be approved by means of a provision of the Agency.

2. Providers of public electronic communications networks or publicly available electronic communications services shall adopt any binding instructions issued by the Agency, including those relating to the measures necessary to remedy a security incident or to prevent its occurrence if a significant threat has been identified.

3. For the purposes of monitoring compliance with Article 40, undertakings providing public communications networks or publicly accessible electronic communications services are required to:

(a) provide the Agency with the information necessary to assess the security of their networks and services, in particular security policy documents; (b) submit to security audits conducted by

the Agency or by an independent qualified body designated by the Agency. The company shall bear the financial burden of the audit.

4. The Agency has the power to investigate cases of non-compliance and their effects on the security of networks and services. Providers of public electronic communications networks or publicly accessible electronic communications services that direct or collect traffic for services offered on national territory are required to provide the information and data necessary for the investigation.

5. The Agency, where appropriate, consults the Authority, the national law enforcement authorities, the Data Protection Authority, and cooperates with them.

6. In the event that the Agency finds failure to comply with this Article and Article 40 or with the implementing provisions set out in paragraphs 1 and 2 by companies providing public communications networks or electronic communications services accessible to the public, the sanctions set out in Article 30, paragraphs 2 to 21, shall apply.».

Notes to Article 43:

— For the text of Article 1 of Legislative Decree No. 82 of June 14, 2021, converted, with amendments, by Law No. 109 of August 4, 2021, as amended by this decree, see the notes to Article 2.

- The text of art. 7 of the aforementioned Legislative Decree no. 82 of 14 June 2021, as amended by this decree, is reported: « Art. 7.

Functions of the National Cybersecurity Agency 1. The agency: (Omitted).

d) is the

competent

National NIS Authority and the Single NIS Contact Point referred to in Article 2, paragraph 1, letters d) *and* e) , *of the NIS Legislative Decree, to protect the legal unity of the system ; d* -bis) *is the National Cybercrisis Management*

Authority of
referred to in Article 2, paragraph 1, letter g) *of the NIS legislative decree ;*

d -ter) *is the national CSIRT, called CSIRT Italia, referred to in Article 2, paragraph 1, letter* i) , *of the NIS Legislative Decree» ;* (Omitted).

n) develops

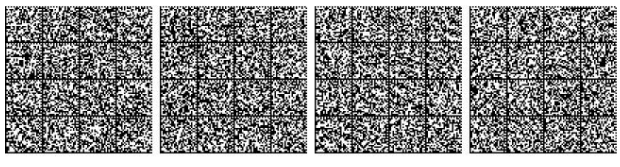
national prevention, monitoring, detection, analysis and response capabilities, to prevent and manage cybersecurity incidents and cyber attacks, including through *CSIRT Italia, referred to in Article 2, paragraph 1, letter i)* of the NIS Legislative Decree. To this end, it promotes public-private partnership initiatives to make these capabilities effective;

n *-bis)* within the scope of the functions referred to in the first sentence of letter *n) ,* carries out all activities aimed at analyzing and providing support for the containment and restoration of the operation of compromised systems, with the collaboration of public or private entities that have suffered IT security incidents or cyber attacks. The failure to cooperate referred to in the first sentence is assessed for the purposes of applying the sanctions provided for in Article 1, paragraphs 10 and 14, of the Perimeter Decree-Law, for the entities referred to in Article 1, paragraph 2 *-bis* of the same Perimeter Decree-Law, the essential entities and *the important entities referred to in Article 6 of the NIS Legislative Decree* and in Article 40, paragraph 3, subparagraph, of the Electronic Communications Code, referred to in Legislative Decree no. 259 of 1 August 2003; State bodies responsible for the prevention, detection and repression of crimes, the protection of public order and safety and the military defence and security of the State, as well as the security intelligence bodies referred to in Articles 4, 6 and 7 of Law No. 124 of 3 August 2007, are excluded;

(Omitted).

1 *-bis* . Also for the purposes of exercising the functions referred to in paragraph 1, letters *r) , s) , t), u) ,* v) , *z)* and *aa) ,* a Technical-Scientific Committee is established within the Agency, with advisory and proposal functions, chaired by the Director General of the same Agency, or by a manager delegated by him, and composed of Agency personnel and qualified representatives of industry, research institutions, academia and associations in the security sector, designated by decree of the President of the Council of Ministers. The composition and organization of the Technical-Scientific Committee are governed according to the methods and criteria defined in the regulation referred to in Article 6, paragraph 1. Participation in the Technical-Scientific Committee does not provide for attendance fees, compensation or reimbursement of expenses.

2. Within the Agency, the national representative and his/her deputy shall be appointed, by decree of the President of the Council of Ministers, to the Governing Board of the European Competence Centre for Cybersecurity in the Industrial, Technology and Research sectors, pursuant to Article 12 of Regulation (EU) 2021/887.



3. (Repealed).

4. The National Evaluation and Certification Center, established at the Ministry of Economic Development, is transferred to the Agency.

5. In accordance with the powers of the Guarantor for the Protection of Personal Data, the Agency, for the purposes set out in this decree, consults and collaborates with the Guarantor, including in relation to incidents involving personal data breaches. The Agency and the Guarantor may enter into specific memoranda of understanding that also define the modalities of their collaboration within the resources available under current legislation and without new or increased burdens on public finances.

— Article 15 of the aforementioned Legislative Decree no. 82 of 14 June 2021, as repealed by this decree, stated: «Art. 15. *(Amendments to the NIS Legislative Decree) ».*

— The text of Article 1 of the aforementioned Legislative Decree no. 105 of 21 September 2019, converted, with amendments, by Law no. 133 of 18 November 2019, as amended by this decree, is reported below:

«Art. 1 *(National cyber security perimeter) .* — 1. – 3. (Omitted).

3 *-bis .* (repealed).

4. – 7. (Omitted).

8. The incident notification pursuant to paragraph 3, letter *a) ,* carried out by the subjects included in the national cyber security perimeter that fall within the scope of the legislative decree transposing Directive (EU) 2022/2555 fulfils the obligations regarding incident notification pursuant to Article 25 of the same legislative decree.

8 -bis *. The obligations set out in Chapter IV and the inspection and sanctioning activities set out in Chapter V for essential entities pursuant to the same legislative decree shall apply to entities included in the national cybersecurity perimeter that are not identified as essential or important entities pursuant to Articles 3 and 6 of the Legislative Decree transposing Directive (EU) 2022/2555, limited to information and network systems other than those included in the list of networks, information systems and IT services referred to in Article 1, paragraph 2, letter* b) *of this decree. The National Cybersecurity Agency, after consulting the inter-ministerial committee for the implementation of the national cybersecurity perimeter,shall establish with its own resolution the terms, methods, specifications and gradual implementation times of the obligations set out in this paragraph* 9. – 16. (Omitted). 17 (repealed).

.

18. – 19 *-ter* . (Omitted).».

Notes to Article 44:

— The text of Article 1, paragraphs 512 to 520, of Law No. 208 of 28 December 2015 (Provisions for the preparation of the annual and multi-year State budget, 2016 Stability Law), published in the *Official Journal* No. 302 of 30 December 2015, is reported below: «512. In order to ensure the optimization and

rationalization of purchases of IT and connectivity goods and services, without prejudice to the centralized acquisition obligations established for goods and services by current legislation, public administrations and companies included in the consolidated income statement of the public administration, as identified by the National Institute of Statistics (ISTAT) pursuant to Article 1 of Law No. 208 of 31 December 2009, 196, procure their supplies exclusively through the purchasing and negotiation tools of Consip Spa or the aggregators, including the regional purchasing bodies, for the goods and services available from these entities. The regions are authorized to hire personnel strictly necessary to ensure the full functionality of the aggregators referred to in Article 9 of Legislative Decree no. 66 of 24 April 2014, converted, with amendments, by Law no. 89 of 23 June 2014, in derogation of the hiring constraints established by current legislation, within the limits of the financing deriving from the Fund referred to in paragraph 9 of the same Article 9 of Legislative Decree no. 66 of 2014.

513. The Agency for Digital Italy (Agid) prepares the three-year plan for information technology in public administration, which is approved by the President of the Council of Ministers or by the delegated Minister.
The Plan contains, for each administration or category of administrations, the list of IT and connectivity goods and services and the related costs, divided into expenses to be incurred for innovation and expenses for current management, also identifying the goods and services whose acquisition is of particular strategic importance.

514. For the purposes of paragraph 512, Consip SpA or the interested aggregator, having consulted AgID for the acquisition of strategic goods and services indicated in the Three-Year Plan for Information Technology in Public Administration referred to in paragraph 513, plans the purchase of IT and connectivity goods and services, consistent with the aggregate demand referred to in the aforementioned Plan. Agid, Consip SpA, and the aggregators, based on analyses of the information in their possession relating to contracts for the purchase of IT goods and services, propose to the administrations and companies referred to in paragraph 512 initiatives and measures, including organizational and process-related ones, aimed at containing expenditure. Consip SpA and the other aggregators promote the aggregation of demand functional to the use of the tools made available to public administrations on a national, regional, or joint basis between multiple administrations.

514 *-bis* . For goods and services whose acquisition is of particular strategic importance as indicated in the Three-Year Plan referred to in paragraph 513, central and local state administrations, with the exception of institutes and schools of all levels, educational institutions and universities, as well as national public social security and welfare bodies and the tax agencies referred to in Legislative Decree no. 300 of 30 July 1999, shall use Consip Spa, within the framework of the Public Administration Procurement Rationalization Program of the Ministry of Economy and Finance.

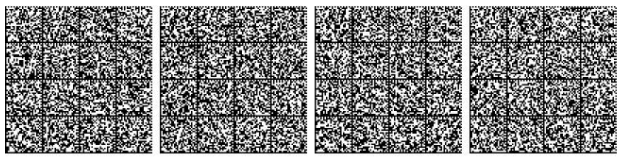
To this end, Consip Spa can support the entities referred to in the previous paragraph in identifying specific interventions to simplify, innovate, and reduce the costs of administrative processes. For the activities referred to in this paragraph, an increase in the funding earmarked for the Ministry of Economy and Finance's Public Administration Procurement Rationalization Program is envisaged: €3,000,000 for 2017, €7,000,000 for 2018, €4,300,000 for 2019, and €1,500,000 annually starting in 2020.

515. The procedure referred to in paragraphs 512 and 514 has an annual expenditure saving target, to be achieved by the end of the three-year period 2016-2018, equal to 50 percent of the average annual expenditure for the current management of the IT sector alone, relating to the three-year period 2013-2015, net of fees for connectivity services and expenditure incurred through Consip SpA or the aggregators documented in the three-year plan referred to in paragraph 513, including that relating to acquisitions of particular strategic importance referred to in paragraph 514 *-bis* as well as through the company referred to in Article 83, paragraph 15, of Legislative Decree no. 112 of 25 June 2008, converted, with amendments, by Law no. 133 of 6 August 2008. Entities governed by Law no. 133 of 9 March 1989 are excluded from the aforementioned savings objective. 88, as well as, for the services provided to the contracting administrations, the company referred to in Article 83, paragraph 15, of Legislative Decree No. 112 of 25 June 2008, converted, with amendments, by Law No. 133 of 6 August 2008, the company referred to in Article 10, paragraph 12, of Law No. 146 of 8 May 1998, and Consip SpA, as well as the administration of justice in relation to the investment expenditures necessary to complete the computerization of civil and criminal proceedings in judicial offices. The savings resulting from the implementation of this paragraph shall be used by the same administrations primarily for investments in technological innovation.

515 *-bis* In order to facilitate participation in Community programs, the public administrations referred to in paragraph 510 may, outside the procedures set forth in paragraph 512 and subsequent paragraphs, request access to the GARR network for research, education, training, and cultural activities, as the only national research network and part of the European research network GEANT, pursuant to Article 40, paragraph 6, of Law No. 166 of August 1, 2002. The related costs are not included in the calculation of annual IT expenditure. The procurement procedure follows the provisions of paragraph 516.

516. The administrations and companies referred to in paragraph 512 may proceed with procurement outside the methods set forth in paragraphs 512 and 514 exclusively following specific, reasoned authorization from the administrative head body, if the goods or services are not available or suitable to meet the administration's specific needs or in cases of necessity and urgency that are in any case essential to ensuring the continuity of administrative management. Procurement carried out pursuant to this paragraph shall be communicated to the National Anti-Corruption Authority and AgID.

517. Failure to comply with the provisions of paragraphs 512 to 516 shall be relevant for the purposes of disciplinary liability and damage to the treasury.



518. Paragraph 3 *-quinquies* of Article 4 of Legislative Decree No. 95 of 6 July 2012, converted, with amendments, by Law No. 135 of 7 August 2012, is repealed.

519. In the acquisition of goods and services referred to in paragraphs 512 to this paragraph, the constitutional bodies shall adopt the measures appropriate to achieve the savings envisaged in their respective autonomy, according to the methods established in their own legislation.

520. For the purposes referred to in paragraph 512, in order to enable the interoperability of the information systems of the National Health Service bodies national and ensure homogeneity of procurement processes across the country, with an agreement sanctioned by the Permanent Conference for Relations between the State, the Regions and the Autonomous Provinces of Trento and Bolzano, following the opinion of Agid and Consip SpA, uniform criteria are defined for the purchases of IT and connectivity goods and services by the National Health Service entities.».

24G00155

ACTS OF THE CONSTITUTIONAL BODIES

CHAMBER OF DEPUTIES

Convening of Parliament in joint session.

The Chamber of Deputies and the Senate of the Republic are convened, in joint session, on Tuesday 8 October 2024, at 12.30pm with the following

Agenda:

Vote for the election of a judge of the Constitutional Court.

The President of the Chamber of Deputies
LORENZO FONTANA

24A05227

MINISTERIAL DECREES, RESOLUTIONS AND ORDINANCES

MINISTRY OF AGRICULTURE, OF FOOD SOVEREIGNTY AND OF THE FORESTS

DECREE 6 September 2024 .

Recognition of the suitability of the «Agro-service R&S srl» Testing Center to conduct official field trials, aimed at producing efficacy data and determining the amount of pesticide residues.

THE DIRECTOR
OF THE CENTRAL PHYTOSANITARY SERVICE

Having seen Legislative Decree no. 194 of 17 March 1995, which, in implementation of Directive 91/414/EEC, regulates the placing on the market of plant protection products;

Having seen in particular paragraphs 5, 6, 7 and 8 of art. 4 of the aforementioned Legislative Decree no. 194/1995;

Having seen the decree of the Minister of Health of 28 September 1995 which modifies Annexes II and III of the aforementioned Legislative Decree no. 194/1995;

Having seen the inter-ministerial decree of 27 November 1996 which, in implementation of the aforementioned Legislative Decree no. 194/1995, regulates the principles of good practice for carrying out field trials and defines the requirements necessary for the official recognition of suitability to conduct pro-

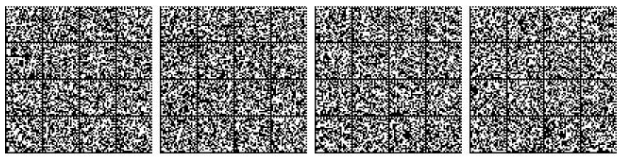
field operations aimed at registering plant protection products; Having seen

Legislative Decree No. 300 of July 30, 1999, reforming the government organization pursuant to Article 11 of Law No. 59 of March 15, 1997;

Having seen Legislative Decree No. 165 of March 30, 2001, containing general provisions on the organization of work within public administrations; Having seen Article 3 of

Legislative Decree No. 173 of November 11, 2022, converted with amendments by Law No. 16 of December 16, 2022; 204, containing "Urgent provisions regarding the reorganisation of the powers of the Ministries" pursuant to which the Ministry of Agricultural, Food and Forestry Policies takes the name of "Ministry of Agriculture, Food Sovereignty and Forestry", in particular paragraph 3 which provides that the names "Minister of Agriculture, Food Sovereignty and Forestry" and "Ministry of Agriculture, Food Sovereignty and Forestry" replace, for all purposes and wherever present, the names "Minister of Agricultural, Food and Forestry Policies" and "Ministry of Agricultural, Food and Forestry Policies";

Having seen the decree of the President of the Council of Ministers of 16 October 2023, no. 178, concerning the "Regulation containing the reorganization of the Ministry of Agriculture, Food Sovereignty and Forestry pursuant to art. 1, paragraph 2, of Legislative Decree no. 44 of 22 April 2023, converted, with amendments, by Law no. 21 June 2023,



n. 74" published in the *Official Journal* n. 285 of 6 December 2023; Having seen the

decree of the Minister of Agriculture, Food Sovereignty and Forests of 31 January 2024, n. 47783, registered at the Court of Auditors on 23 February 2024, under n. 288, with which the non-general management offices and their relative responsibilities were identified;

Having seen the directive of the Minister of Agriculture, Food Sovereignty and Forestry, ref. no. 45910 of 31 January 2024, registered at the Court of Auditors on 23 February 2024, under no. 280, containing the general guidelines on administrative activity and management for 2024;

Having seen the request submitted on 12 March 2024 by the Test Centre «Agroservice R&S srl» with operational headquarters in contrada Papparicotta snc - 76123 Andria (BT); Having seen the

directive of the Head of the Department of the Common Agricultural Policy and Rural Development prot. no. 64727 of 9 February 2024, registered at the UCB on 7 March 2024, at no. 168, for the implementation of the objectives defined by the Minister of Agriculture, Food Sovereignty and Forests prot. no. 45910 of 31 January 2024; Having seen the directive of the Director General of

Rural Development no. 108781 of 5 March 2024, registered at the UCB on 12 April 2024 at no. 260, which assigned objectives to managers and the financial and human resources for their achievement for the year 2024;

Having seen the directorial decree prot. no. 0193251 of 30 April 2024, by which Dr. Bruno Caio Faraglia, second-level manager, was conferred the position of director of the non-general management office DISR V - Central Phytosanitary Service, Plant Production - of the General Directorate for Rural Development of the Department of the Common Agricultural Policy and Rural Development; Having seen the minutes no. 0414000 of 5 September 2024, relating to the compliance

audit carried out on 31 August 2024 by the inspection team appointed with note no. 0254399 of 6 June 2024;

Considering that the aforementioned center has declared that it meets the requirements of the current legislation, as of March 12, 2024, on the basis of the appropriate documentation submitted; Considering the favorable

outcome of the verification of compliance to carry out field trials for registration purposes, aimed at producing efficacy data and determining the amount of pesticide residues, carried out at the "Agroservice R&S srl" Center;

Decrees:

Art. 1.

1. The «Agroservice R&S srl» Centre with operational headquarters in contrada Papparicotta snc - 76123 Andria (BT), is recognised as a suitable test centre for carrying out official field trials with plant protection products aimed at obtaining the following information: *a)* identification of degradation and

reaction products of metabolites in treated plants or products (Annex II, point 6.1);

(b) evaluation of the behaviour of residues of the active substances and their metabolites from application until the time of harvesting or marketing of the stored products (Annex II, point 6.2);

(c) definition of the general balance of residues of the active substances

(Annex II, point 6.3); (d) tests for the determination of residues of active substances in the various environmental

compartments; *(e)* determination of residues in or on treated products, foodstuffs or feed (Annex III, point

8.1); (f) environmental and ecotoxicological field tests suitable for the evaluation of the fate and behaviour in the environment of the active

substances and their metabolites (Annex II, Part A, point 8.3); (g) evaluation of data on residues in subsequent crops

successive or rotational (Annex III, point 8.5);

h) identification of waiting times for jobs pre- or *post* -harvest (Annex III, point 8.6).

2. The recognition referred to in paragraph 1 concerns field trials of efficacy and the determination of the amount of pesticide residues in the following sectors of activity: *a)* non-agricultural areas; *b)* tree crops; *c)*

herbaceous crops; *d)* forestry

crops; *e)* ornamental

crops; *f)* horticultural

crops; *g)* seed

treatment; *h) post* -harvest

conservation ; *i)* weed

control; *j)* entomology;

k) nematology; *l)* plant pathology.

Art. 2.

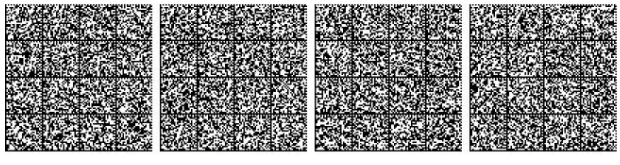
1. Maintaining the suitability referred to in Article 1 is subject to periodic and regular checks of compliance with the required requirements by inspectors registered in the specific national list referred to in Article 4, paragraph 8, of the aforementioned Legislative Decree no. 194/1995.

2. The "Agroservice R&S srl" Testing Center is required to communicate to this Ministry the precise indication of the types of tests it will perform, as well as their territorial location.

3. The aforementioned center is also required to communicate any changes that may occur with respect to what it declared in the recognition application, as well as to what is provided for in this decree.

Art. 3.

1. The recognition of suitability, referred to in Article 1 of this decree, is valid from the date of inspection, carried out on August 31, 2024, until December 31, 2026.



2. If the "Agroservice R&S srl" Testing Center intends to confirm or change the operational areas referred to in this decree, it may submit a specific request, accompanied by the relevant documentation proving possession of the required requisites, no later than February 2026.

This decree, pursuant to Article 13 of Legislative Decree No. 196/2003, will be published in compliance with the legal obligations set forth in Legislative Decree No. 33/2013 and published in the *Official Journal* of the Italian Republic.

Rome, September 6, 2024

The director: FARAGLIA

24A05071

DECREE 6 September 2024 .

Recognition of the suitability of the «Bayer CropScience srl» Testing Center to carry out official field trials, aimed at producing efficacy data and determining the extent of pesticide residues.

THE DIRECTOR
OF THE CENTRAL PHYTOSANITARY SERVICE

Having seen Legislative Decree no. 194 of 17 March 1995, which, in implementation of Directive 91/414/EEC, regulates the placing on the market of plant protection products;

Having seen in particular paragraphs 5, 6, 7 and 8 of art. 4 of the aforementioned Legislative Decree no. 194/1995;

Having seen the decree of the Minister of Health of 28 September 1995 amending Annexes II and III of the aforementioned Legislative Decree no. 194/1995; Having seen

the interministerial decree of 27 November 1996 which, in implementation of the aforementioned Legislative Decree no. 194/1995, regulates the principles of good practice for carrying out field trials and defines the requirements necessary for official recognition of suitability for conducting field trials aimed at registering plant protection products; Having seen Legislative Decree no. 300 of 30 July 1999,

reforming the government organization pursuant to art. 11 of Law no. 59 of 15 March 1997;

Having seen Legislative Decree No. 165 of 30 March 2001, containing general rules on the organisation of work within public administrations; Having seen Article 3 of Legislative

Decree No. 173 of 11 November 2022, converted with amendments by Law No. 204 of 16 December 2022, containing «Urgent provisions regarding the reorganisation of the powers of the Ministries» pursuant to which the Ministry of Agricultural, Food and Forestry Policies

assumes the name of «Ministry of Agriculture, Food Sovereignty and Forests», in particular paragraph 3 which provides that the names

«Minister of Agriculture, Food Sovereignty and Forests» and «Ministry of Agriculture, Food Sovereignty and Forests» replace,

for all intents and purposes and wherever present, the names "Minister of Agricultural, Food and Forestry Policies" and "Ministry of Agricultural, Food and Forestry Policies";

Having seen the Prime Ministerial Decree of 16 October 2023, no. 178, concerning the "Regulation concerning the reorganization of the Ministry of Agriculture, Food Sovereignty and Forestry pursuant to Article 1, paragraph 2, of Legislative Decree no. 44 of 22 April 2023, converted, with amendments, by Law no. 74 of 21 June 2023" published in the *Official Journal* no. 285 of 6 December 2023;

Having seen the decree of the Minister of Agriculture, Food Sovereignty and Forestry of 31 January 2024, no. 47783, registered at the Court of Auditors on 23 February 2024, under no. 288, which identified the non-general management offices and their related responsibilities;

Having seen the directive of the Minister of Agriculture, Food Sovereignty and Forestry, ref. no. 45910 of 31 January 2024, registered at the Court of Auditors on 23 February 2024, under no. 280, containing the general guidelines on administrative activity and management for 2024;

Having seen the application submitted on 18 March 2024 by the Testing Centre «Bayer CropScience srl» with operational headquarters in via Aurelia km 36 - 00055 Ladispoli (RM);

Having seen the directive of the Head of the Department for the Common Agricultural Policy and Rural Development, ref. no. 64727 of 9 February 2024, registered at the UCB on 7 March 2024, under no. 168, for the implementation of the objectives defined by the Minister of Agriculture, Food Sovereignty and Forestry, ref. no. 45910 of 31 January 2024;

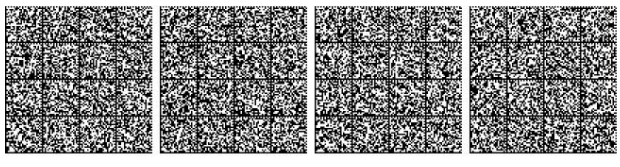
Having seen the directive of the Director General for Rural Development no. 108781 of 5 March 2024, registered at the UCB on 12 April 2024 under no. 260, which assigned the objectives to managers and the financial and human resources for their achievement for the year 2024;

Having seen the directorial decree prot. no. 0193251 of 30 April 2024, by which Dr. Bruno Caio Faraglia, second-level manager, was conferred the position of director of the non-general management office DISR V - Central Phytosanitary Service, Plant Production - of the General Directorate for Rural Development of the Department of the Common Agricultural Policy and Rural Development;

Having seen the report no. 0349807 of 1 August 2024, relating to the compliance check carried out on 18 July 2024 by the inspection team appointed with note no. 0255594 of 7 July 2024;

Considering that the aforementioned center has declared that it possesses the requirements prescribed by the legislation in force, as of March 18, 2024, on the basis of the appropriate documentation presented;

Considering the favorable outcome of the verification of compliance to carry out field trials for registration purposes, aimed at producing efficacy data and determining the amount of pesticide residues, carried out at the "Bayer CropScience srl" Center;



Decrees:

Art. 1.

1. The "Bayer CropScience srl" Centre, with operational headquarters at Via Aurelia km 36 - 00055 Ladispoli (RM), is recognised as a suitable testing centre for carrying out official field trials with plant protection products aimed at obtaining the following information: *a)* efficacy of plant protection products (referred to in Annex III, point 6.2 of Legislative Decree no. 194/1995); *b)* data on the appearance or possible development of resistance (referred to in Annex III, point 6.3 of Legislative Decree no. 194/1995); *c)* impact on quantitative and/or qualitative yield (referred to in Annex III, point 6.4 of Legislative Decree no. 194/1995); *d)* phytotoxicity towards target plants and plant products (referred to in Annex III, point 6.5 of Legislative Decree No. 194/1995); *e)* observations regarding undesirable side effects (referred to in Annex III, point 6.6 of Legislative Decree No. 194/1995); *f)* metabolism, distribution and expression of the residue in plants or livestock (referred to in point 8.1 of EC Regulation No. 545/2011); *g)* residue testing (referred to in point 8.2 of EC Regulation No. 545/2011); *h)* definition of the general residue balance of the active substances (referred to in Annex II, point 6.3 of Legislative Decree No. 194/1995 and point 8.6 of EC Regulation No. 545/2011);

i) seed treatment;

j) post -harvest conservation ;

k) weed control;

l) entomology;

m) nematology;

n) plant pathology;

o) agricultural zoology;

p) harmful vertebrates;

q) growth regulators.

Art. 2.

1. Maintaining the suitability referred to in Article 1 is subject to periodic and regular checks of compliance with the required requirements by inspectors registered in the specific national list referred to in Article 4, paragraph 8, of the aforementioned Legislative Decree no. 194/1995.

2. The «Bayer CropScience srl» testing centre is required to communicate to this Ministry the precise indication of the types of tests it will carry out, as well as their territorial location.

3. The aforementioned center is also required to communicate any changes that may occur with respect to what it declared in the recognition application, as well as to what is provided for in this decree.

Art. 3.

1. The recognition of suitability, referred to in Article 1 of this decree, is valid from the date of inspection, carried out on July 18, 2024, until December 31, 2026.

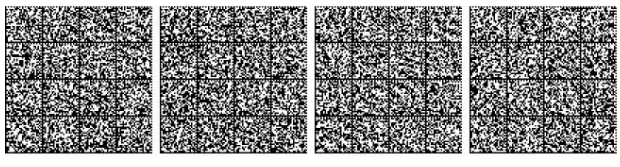
2. If the "Bayer CropScience srl" testing center intends to confirm or change the operational areas referred to in this decree, it may submit a specific request, accompanied by the relevant documentation proving possession of the required requisites, no later than February 2026.

This decree, pursuant to Article 13 of Legislative Decree No. 196/2003, will be published in compliance with the legal obligations set forth in Legislative Decree No. 33/2013 and published in the *Official Journal* of the Italian Republic.

Rome, September 6, 2024

The director: FARAGLIA

24A05072



MINISTRY OF ECONOMY AND FINANCE

DECREE 26 September 2024 .

Issuance of 182-day ordinary Treasury bonds, first and second *tranches* .

THE DIRECTOR GENERAL OF THE TREASURY

Having seen Royal Decree No. 2440 of 18 November 1923, concerning provisions on the administration of the State's assets and general accounting, and in particular Article 71; Having seen Article 548 of the "Regulations

for the administration of the State's assets and general accounting" (hereinafter the "Regulations"), approved by Royal Decree No. 827 of 23 May 1924, as amended by Article 1 of Presidential Decree No. 470 of 21 April 1961; Having seen Presidential Decree No. 30 December 2003; 398, and subsequent amendments, with which the "Consolidated Law of Legislative and Regulatory Provisions

on Public Debt" (hereinafter the "Consolidated Law") was approved, and in particular Article 3, which provides that the Minister of Economy and Finance is authorised, in each financial year, to issue framework decrees which allow, among other things, the Treasury to carry out borrowing operations on the domestic or foreign market in the form of short-, medium- and long-term financial products and instruments, indicating the nominal amount, the interest rate or the criteria for its determination, the duration, the minimum amount that can be subscribed, the placement system and any other characteristics and methods;

Having seen Ministerial Decree No. 5048315 of 15 December 2023, issued pursuant to Article 3 of the "Consolidated Law" (hereinafter the "framework decree"), which defines for the 2024 financial year the objectives, limits and methods to which the Treasury Department must adhere in carrying out the financial transactions referred to in the same article, providing that the transactions themselves be ordered by the Director General of the Treasury or, by his delegation, by the Director of Directorate II of the same Department and that, in the event of the absence or impediment of the latter, the aforementioned transactions may be ordered by the same Director General of the Treasury, even in the presence of continuous delegation; Having seen Decree No. 216 of 22 December 2009 and in particular Article 23 relating

to operators "Specialists in Italian government bonds" (hereinafter "Specialists"); Having seen the management decree no. 993039 of 11 November 2011 (Management Decree on Specialists), concerning the "Selection and Evaluation of Specialists in

Government Bonds" and subsequent amendments and additions;

Having seen the legislative decree of 1 April 1996, n. 239, and subsequent amendments and additions;

Having seen Legislative Decree no. 461 of 21 November 1997, and subsequent amendments and additions, containing provisions for the reorganisation of the legislation on capital income and other income;

Having regard to Articles 4 and 11 of the Consolidated Law, regarding the dematerialization of government

bonds; Having regard to Articles 24 et seq. of the Consolidated Law, regarding the centralized management of

government bonds; Having regard to Ministerial Decree No. 143 of 17 April 2000, which adopted the regulation concerning the regulation of the centralized management of government bonds;

Having seen the directorial decree of 23 August 2000, by which the centralized management service for government bonds was entrusted to Monte Titoli Spa (now *Euronext Securities Milan);* Having seen

Article 17 of the Consolidated Law, relating to the admissibility of the facsimile reproduction service in participation in government bond auctions;

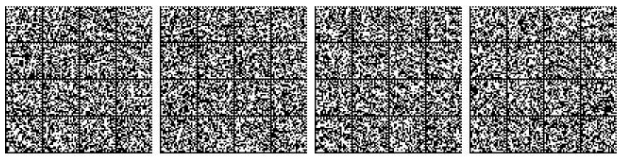
Having regard to Ministerial Decree No. 3088 of 15 January 2015, establishing rules for transparency in the placement of government bonds; Having regard to Regulation (EU)

No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012, as subsequently amended by Regulation (EU) No. 2023/2845 of the European Parliament and of the Council of 13 December 2023 as regards settlement discipline, the provision of cross-border services, supervisory cooperation, the provision of banking-type ancillary services and requirements for third-country central securities depositories, and as supplemented by Commission Delegated Regulation (EU) No 2017/389 of 11 November 2016 as regards the parameters for the calculation of financial penalties for settlement fails and the operations of central securities depositories (CSDs) in host Member States and by Commission Delegated Regulation (EU) No 2018/1229 of 25 May 2018 as regards regulatory technical standards on settlement discipline, as amend ... 2021/70 of the Commission of 23 October 2020 with reference to the entry into force thereof, by Commission Delegated Regulation (EU) No. 2022/1930 of 6 July 2022 as regards the date of application of the provisions relating to the buy-in procedure and, lastly, by Commission Delegated Regulation (EU) No. 2023/1626 of 19 April 2023 as regards the penalty mechanism for settlement fails relating to cleared transactions that central

counterparties submit for settlement purposes;

Having regard to Ministerial Decree No. 12953 of February 17, 2023, concerning the "Accounting provisions in the event of delays in the settlement of issuance, exchange, and repurchase transactions of government bonds, as well as repurchase agreements conducted by the Ministry of Economy and Finance"; Having regard to Law No. 213 of December 30, 2023, containing

the "State budget forecast for the 2024 financial year and the multi-year budget for the three-year period 2024-2026", and in particular Article 3, paragraph 2, which establishes the maximum limit for issuing public loans for that year; Having regard to the guidelines for managing public debt for 2024;



Having seen Resolution No. 101204 of November 23, 2023, by which the Director General of the Treasury delegated, effective January 1, 2024, the General Manager Head of Directorate II with regard to the responsibilities relating to public debt, pursuant to the aforementioned Article 3 of Presidential Decree No. 398/2003, in order to ensure the continuity and timeliness of administrative action;

Considering the need to conduct auctions of Treasury bills with bids from eligible operators expressed in terms of yield, rather than price, in accordance with the prevailing practice on euro area money markets; Considering that the amount of issues arranged up to 23 September 2024,

net of public loan repayments already made, amounts to €97,284 million;

Decrees:

Art. 1.

Pursuant to and for the purposes of Article 3 of the Consolidated Law and the Framework Decree, and in derogation from Article 548 of the Regulation, the issue of a first *tranche* of ordinary Treasury bonds (hereinafter referred to as *BOTs)* is arranged for 30 September 2024 , with a maturity of one hundred and eighty-two days and maturing on 31 March 2025, up to a maximum nominal value of 7,000 million euros.

For this issue, it is possible to reopen in *tranches.*

.

At the end of the allocation procedure, the issuance of an additional placement of the BOTs referred to in this decree is also ordered.

Art. 2.

Bids placed at yields lower than the "minimum acceptable yield", determined according to the following methods, are automatically excluded from the auction: *a)* if total demand exceeds supply, the

weighted average yield of the bids is determined which, ordered starting from the lowest yield, constitute the second half of the nominal amount being issued; if total demand is lower than supply, the weighted average yield of the bids is determined which, ordered starting from the lowest yield, constitute the second half of the amount asked;

b) the minimum acceptable yield is identified, corresponding to the weighted average yield referred to in point *a)* reduced by 50 basis points (1 percentage point = 100 basis points).

In the event of exclusion pursuant to the first paragraph of this Article, the weighted average award yield is determined by subtracting from the total quantity offered by the issuer a quantity equal to the excluded quantity.
Excluded bids are assigned a yield equal to the higher of the yield obtained by subtracting 10 basis points from the minimum yield accepted in the auction and the minimum acceptable yield.

Art. 3.

Requests made at yields more than 100 basis points higher than the weighted average yield of requests that, ranked from lowest to highest, represent half of the total amount received are excluded from allocation. If this amount exceeds the *tranche* offered, the weighted average yield is calculated based on the total amount of requests, ranked in ascending order by yield and equal to half of the *tranche* offered.

Requests excluded pursuant to Article 2 of this decree are excluded from the calculation of the weighted average yield referred to in this Article.

Art. 4.

Once the auction operations have been completed, a subsequent decree will indicate the minimum acceptable yield and the maximum acceptable yield - deriving from the mechanisms referred to in Articles 2 and 3 of this decree - and the weighted average award yield, as well as the corresponding weighted average price.

In the event of issuance of *tranches* subsequent to the first, the decree referred to in the previous paragraph will also report the weighted average price determined for tax purposes, pursuant to Article 17 of this decree.

Art. 5.

BOTs are subscribed for a minimum amount of 1,000 euros and the subscribed amounts are represented by accounting entries in favor of the entitled parties.

The Bank of Italy automatically enters the BOTs subscribed at auction to be settled into the clearing and settlement service for financial instruments with a value date equal to the settlement date. To settle the assigned BOTs, the operator participating in the auction may use another intermediary, to be notified to the Bank of Italy, in accordance with the regulations and procedures established by the Bank.

Based on the allocations, the successful intermediaries credit the relevant amounts to the accounts held with the subscribers.

Art. 6.

By way of derogation from the provisions of the aforementioned Article 548 of the Regulation, the duration of BOTs may be expressed in "days".

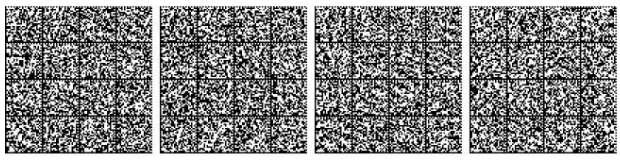
The calculation of days for the purposes of determining the expiry date starts from the day following the settlement of the BOTs.

Art. 7.

Both specialist operators and aspiring specialists can participate in the auction.

Both specialists and aspirants participate on their own behalf and on behalf of others.

The Bank of Italy is authorized to stipulate specific agreements with operators
specialists and with the operators notified by the Ministry of Economy and Finance who intend to advance



application for registration in the list of specialists, to regulate participation in auctions via the national interbank network.

The Bank of Italy, as manager of the provincial treasury service of the State, is entrusted with the execution of the operations.

Art. 8.

Purchase requests from operators admitted to participate in the auctions must be formulated in terms of yield, which may be positive, zero, or negative. These yields are considered gross and expressed on a simple capitalization basis over a three hundred and sixty-day year.

Dealers' requests must be submitted via the national interbank network and must indicate both the amount of BOTs they intend to subscribe for and the related yield. Requests without an indication of the yield will not be accepted at the auction.

The yields indicated by operators at auction, expressed as percentages, may vary by one thousandth of a percentage point or a multiple thereof. Any variations of a different amount are rounded down.

The amount of each request cannot be less than 1,500,000 euros of nominal capital.

Requests from each operator indicating an amount that exceeds, even as a total sum of them, the amount offered by the Treasury will be taken into consideration starting from the one with the lowest yield and up to the amount offered, except as established in Articles 2 and 3 of this decree.

Requests for amounts that are not multiples of the minimum subscribable amount referred to in Article 5 will be rounded down.

Any offers indicating that exchange securities are to be paid in settlement of the securities being issued will not be taken into consideration.

Art. 9.

Requests from each individual operator, to be addressed to the Bank of Italy, must be transmitted using the national interbank network according to the technical methods established by the Bank of Italy itself.

To ensure the integrity and confidentiality of data transmitted through the national interbank network, bilateral authentication and encryption keys are exchanged between operators and the Bank of Italy.

If it is not possible to send messages to the network due to equipment malfunction, requests to participate in the auction must be sent using a form to be transmitted to the Bank of Italy, in accordance with the agreements referred to in Article 7, paragraph 3, of this decree.

Art. 10.

Purchase requests must reach the Bank of Italy no later than 11:00 a.m. on September 26, 2024. Requests not received by this deadline will not be considered.

Any requests replacing those already received will be considered only if received within the deadline indicated above.

Requests can no longer be withdrawn after the aforementioned deadline.

Art. 11.

The auction operations are carried out by the Bank of Italy, after the expiry of the deadline referred to in the previous article, in the presence of a representative of the Bank itself and with the intervention, also through electronic communication systems, of a representative of the Ministry of Economy and Finance, who acts as a notarizing officer and draws up a specific report in which the award yields and the amount of the related passive or active interest, determined by the difference between 100 and the corresponding award prices, must be highlighted for each tranche.

In the event of extraordinary events, the Bank of Italy and the Ministry of Economy and Finance, in derogation from the provisions of the previous paragraph, each within their respective competences, may choose to conduct the auction operations relating to the security subject to this issue remotely using IT tools, based on methods agreed upon by the two institutions.

Art. 12.

The State Treasury sections are authorized to account for the amount of interest in a specific single summary document for each *tranche* issued and to issue – on the same day established for the issuance of BOTs by this decree – receipts for the nominal amount issued.

The expenditure for passive interests will be charged to chapter 2215 (voting unit 21.1) of the expenditure forecast of the Ministry of Economy and Finance for the financial year 2025 or to the corresponding ones for the same year.

Interest income will be charged to Chapter X, Section 3240, Article 3 (voting unit 2.1.93), with value date equal to the settlement date of the securities indicated in Article 1, paragraph 1 of this decree. Upon payment, the competent State Treasury section will issue a specific receipt.

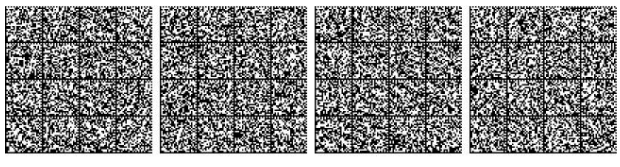
Art. 13.

The allocation of BOTs is carried out at the yield respectively indicated by each operator participating in the auction, who can submit up to five requests each at a different yield.

Art. 14.

The awarding of BOTs is carried out following the increasing order of the yields offered by the operators, up to the amount offered, except as specified in Articles 2 and 3 of this decree.

In the event that the requests made for the maximum yield accepted cannot be fully satisfied, a *pro-rata* distribution will be carried out .



The successful bids are settled at the prices corresponding to the yields indicated by the operators.

Art. 15.

Once the assignment operations have been completed, the supplementary placement of the aforementioned securities, referred to in Article 1 of this decree, will begin, for an amount equal to 10% of the nominal amount offered in the ordinary auction.

This *tranche* is reserved exclusively for specialists who participated in the ordinary *tranche* auction with at least one bid placed at a yield no higher than the maximum acceptable yield referred to in Article 3 of this decree. These specialists may participate in the supplementary placement by submitting subscription applications until 3:30 PM on September 27, 2024.

Offers not received by this deadline will not be considered. not taken into consideration.

The supplementary placement takes place at the weighted average auction allotment yield of the *tranche* ordinary; any requests made at a different yield are awarded at the described weighted average yield.

For the purposes of the allocation, the provisions of Articles 5 and 11 shall apply, where applicable. The request of each specialist must be submitted according to the procedures set out in Articles 9 and 10 and must contain an indication of the amount of the securities to be subscribed.

Each request cannot be less than €1,500,000; any requests for a lower amount will not be considered.

Each request cannot exceed the entire amount offered in the supplementary placement; any requests for a higher amount are accepted up to the limit of the amount offered in the supplementary placement. same.

Requests for amounts that are not multiples of the minimum subscribable amount referred to in Article 5 will be rounded down.

Any offers indicating that exchange securities are to be paid in settlement of the securities being issued will not be taken into consideration.

Art. 16.

The amount that is rightfully due to each specialist in the additional placement is determined as follows:

a) for an amount equal to 5% of the nominal amount offered in the ordinary auction, is equal to the ratio between the value of the securities for which the specialist was awarded in the last three ordinary auctions of six-month BOTs, including the ordinary auction immediately preceding the reopening itself, and the total assigned in the same auctions to the same specialists admitted to participate in the supplementary placement; the amounts assigned according to the methods set out in Article 2 of this decree do not contribute to determining the amount due to each specialist; *b)* for a further amount equal to 5% of the nominal amount offered in the ordinary auction, is

assigned on the basis of the evaluation, carried out by the Treasury, of the performance relating to the same specialists, recorded on a quarterly basis.

on the wholesale trading venues selected pursuant to Article 23, paragraphs 10, 11, 13, and 14, of the Decree of the Minister of Economy and Finance of 22 December 2009, No. 216, cited in the preamble; this assessment is communicated to the Bank of Italy and to the specialists themselves.

Requests are satisfied by assigning each specialist, as a priority, the lower of the requested amount and the amount legally due. If one or more specialists submit requests lower than their legally due amount, or have not submitted any requests at all, the difference is assigned to the operators who have submitted requests higher than their legally due amount. The assignment is made based on the quotas referred to in the previous letters *a)* and *b)* .

The settlement of the securities subscribed in the supplementary placement is carried out by the assigned operators on the same day as the settlement of the securities assigned in the ordinary auction indicated in Article 1, paragraph 1 of this decree.

Art. 17.

The amount of interest deriving from BOTs is paid in advance and is determined, for tax purposes only, with reference to the weighted average price - expressed with rounding to the third decimal place - corresponding to the weighted average yield of the first *tranche.* .

Without prejudice to the provisions in force regarding tax exemptions on public debt, the provisions of Legislative Decree No. 239 of 1 April 1996, as amended, and Legislative Decree No. 461 of 21 November 1997, as amended, shall apply to the BOTs issued under this decree.

This decree will be published in the *Official Journal* of the Italian Republic.

Rome, September 26, 2024

p. The Director General of the Treasury: IACOVONI

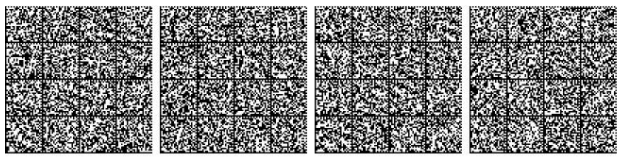
24A05110

DECREE 27 September 2024 .

Reopening of subscription operations for 3.00% multi-year Treasury bonds, with accrual starting on 1 February 2019 and maturing on 1 August 2029, seventeenth and eighteenth *tranches* .

THE GENERAL DIRECTOR
OF THE TREASURY

Having seen the Presidential Decree of 30 December 2003, no. 398, and subsequent amendments, with which the "Consolidated Law of Legislative and Regulatory Provisions on Public Debt" (hereinafter the "Consolidated Law") was approved, and in particular Article 3, which provides that the Minister of Economy and Finance is authorised, in each financial year, to issue framework decrees which allow, among other things, the Treasury to carry out borrowing operations on the domestic or foreign market in the form of short-term financial products and instruments,



long-term, indicating the nominal amount, the interest rate or the criteria for its determination, the duration, the minimum amount that can be subscribed, the placement system and any other characteristics and methods;

Having regard to Decree No. 101633 of 19 December 2022 (hereinafter the "General Decree") and subsequent amendments and additions, which continuously establishes the characteristics and issuance procedures for medium- and long-term government bonds to be placed through auction; Having regard to Ministerial Decree No. 5048315 of 15

December 2023, issued pursuant to Article 3 of the "Consolidated Law" (hereinafter "framework decree"), which defines for the financial year 2024 the objectives, limits and methods that the Treasury Department must adhere to in carrying out the financial transactions referred to in the same article, providing that the transactions themselves be ordered by the Director General of the Treasury or, by his delegation, by the Director of the Second Directorate of the same Department and that, in the event of the absence or impediment of the latter, the aforementioned transactions may be ordered by the same Director General of the Treasury, even in the presence of continuous delegation; Having seen Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014, on improving securities

settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012, as subsequently amended by Regulation (EU) No. 2023/2845 of the European Parliament and of the Council of 13 December 2023 as regards settlement discipline, the provision of cross-border services, supervisory cooperation, the provision of banking-type ancillary services and requirements for third-country central securities depositories, and as supplemented by Commission Delegated Regulation (EU) No. 2017/389 of 11 November 2016 as regards the parameters for the calculation of financial penalties for settlement fails and the operations of central securities depositories (CSDs) in host Member States and by Commission Delegated Regulation (EU) No. 2018/1229 of 25 May 2018 as regards regulatory technical standards on settlement discipline, as amended by Commission Delegated Regulation (EU) No. 2021/70 of the Commission of 23 October 2020 with reference to the entry into force thereof, by Commission Delegated Regulation (EU) No. 2022/1930 of 6 July 2022 as regards the date of application of the provisions relating to the buy-in procedure and, lastly, by Commission Delegated Regulation (EU) No. 2023/1626 of 19 April 2023 as regards the penalty mechanism for settlement fails relating to cleared transactions that central counterparties submit for settlement purposes;

Having seen Ministerial Decree No. 12953 of 17 February 2023, concerning the "Accounting provisions in the event of delays in the settlement of transactions involving the issuance, exchange and repurchase of government bonds, as well as in repurchase agreements carried out by the Ministry of Economy and Finance"; Having seen Ministerial Decree No. 96718 of 7

December 2012, concerning the "Provisions for the separation, negotiation and reconstitution of the compo-

coupon rates, the inflation-indexed component and the nominal redemption value of government bonds *(stripping) »;* Having seen Law No. 213

of 30 December 2023, containing the «State budget forecast for the financial year 2024 and the multi-year budget for the three-year period 2024-2026», and in particular Article 3, paragraph 2, which established the maximum limit for issuing public loans for the same year;

Considering that the amount of the issues arranged up to 24 September 2024, net of repayments of public loans already made, amounts to 97,284 million euros;

Having seen Resolution No. 101204 of November 23, 2023, by which the Director General of the Treasury delegated, effective January 1, 2024, the General Manager Head of Directorate II with regard to the responsibilities relating to public debt, pursuant to the aforementioned Article 3 of Presidential Decree No. 398/2003, in order to ensure the continuity and timeliness of administrative action;

Having seen its decrees dated 26 February, 27 March, 29 April, 29 May, 26 June and 29 July 2019, the decree of 18 May 2021 relating to the establishment of securities for the repurchase agreement operations of the Ministry of Economy and Finance (REPO), as well as of 16 June 2021 and 13 April 2022, with which the issue of the first sixteen *tranches* of 3.00% multi-year Treasury bonds with accrual date 1 February 2019 and maturity 1 August 2029 was ordered;

Having deemed it appropriate, in relation to market conditions, to arrange for the issuance of a seventeenth *tranche* of the aforementioned multi-year Treasury bonds;

Decrees:

Art. 1.

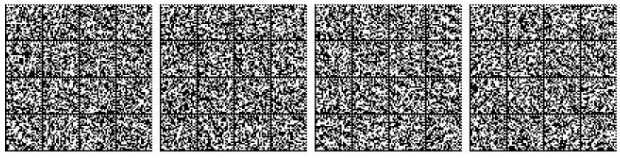
Pursuant to and for the purposes of Article 3 of the "Consolidated Law" and the "Framework Decree", the issuance of a seventeenth *tranche* of 3.00% multi-year Treasury bonds is hereby ordered, with accrual starting on February 1, 2019 and expiring on August 1, 2029. The issuance of the aforementioned *tranche* It is provided for a nominal amount between a minimum of 750 million euros and a maximum of 1,000 million euros.

The bonds bear gross annual interest of 3.00%, payable in two semi-annual installments in arrears, on February 1st and August 1st of each year of the loan term.

The first eleven coupons of the bonds issued with this decree, having arrived at the expiry date, will not be paid.

On the same bonds, operations can be carried out to separate and reconstitute the coupon components from the redemption value of the security *("coupon stripping").*

The characteristics and methods of issuing the aforementioned securities are those defined in the "general decree", which is hereby deemed to be fully referred to and to which reference is made for anything not expressly provided for in this decree.



Art. 2.

Operators' bids for the *tranche* referred to in Article 1 of this decree must be received by 11:00 a.m. on September 27, 2024, in compliance with the procedures set forth in Articles 7, 8, 9, 10, and 11 of the "General Decree."

The placement commission, equal to 0.150% of the subscribed nominal capital, will be paid according to the methods set out in Article 8 of the "General Decree" indicated in the preamble.

Art. 3.

At the end of the allocation operations referred to in the previous article, the placement of the eighteenth *tranche* of the securities themselves takes place, according to the methods indicated in articles 12, 13, 14 and 15 of the "general decree".

The amount of the *tranche* relating to the security subject to this issue will be equal to 20 percent as established by Article 14, paragraph 2, of the "General Decree".

Government bond specialists have the right to participate in the supplementary placement by submitting subscription applications by 3.30 pm on 30 September 2024.

Art. 4.

Settlement of the bonds subscribed at auction and in the supplementary placement will be carried out by the assigned operators on October 1, 2024, at the auction price and with the payment of gross interest for sixty-one days. To this end, the Bank of Italy will automatically enter the related items into the clearing and settlement service with a value date equal to the settlement date.

In the event of delay in the settlement of the securities referred to in this decree, the provisions of Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 and Ministerial Decree No. 12953 of 17 February 2023, cited in the preamble, shall apply.

Art. 5.

On 1 October 2024, the Bank of Italy will pay the proceeds of the bonds assigned at the auction hammer price, together with the 3.00% gross annual interest due to the State, to the Rome Section of the State Treasury.

The aforementioned Treasury section issues, for said payments, separate receipts of income to the State budget, with the amount relating to the proceeds of the issue being charged to Chapter X, Chapter 5100, Article 3 (parliamentary voting units 4.1.171) and to Chapter 3240, Article 3 (parliamentary voting units 2.1.93) for the amount relating to the gross interest due.

Art. 6.

The interest charges relating to the financial years 2025 to 2029, as well as the charge for the repayment of the capital relating to the financial year 2029, will be charged to the items that will be entered in the budget forecast of the expenditure of the Ministry of Economy and Finance for the same years and corresponding, respectively, to chapters 2214 (parliamentary voting units 21.1) and 9502 (parliamentary voting units 21.2) of the budget forecast for the current year.

The amount of the placement commission, provided for in art. 2 of this decree, will be recorded, at each quarterly payment interval, by the Treasury sections among the "payments to be settled" and will be charged to chapter 2247 (parliamentary voting unit 21.1; management code 109) of the expenditure forecast of the Ministry of Economy and Finance for the financial year 2024 or the corresponding year for subsequent years.

This decree will be published in the *Official Journal* of the Italian Republic.

Rome, September 27, 2024

p. The Director General of the Treasury: IACOVONI

24A05138

DECREE 27 September 2024 .

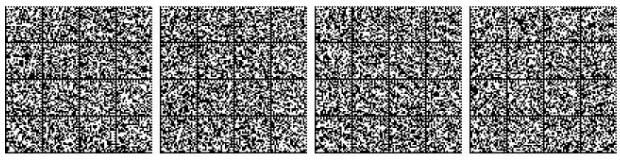
Reopening of subscription operations for 3.85% multi-year Treasury bonds, with accrual beginning on August 1, 2024 and maturity on February 1, 2035, fifth and sixth *tranches* .

THE GENERAL DIRECTOR
OF THE TREASURY

Having seen Presidential Decree No. 398 of 30 December 2003, as amended, approving the "Consolidated Law on Legislative and Regulatory Provisions on Public Debt" (hereinafter the "Consolidated Law"), and in particular Article 3, which provides that the Minister of Economy and Finance is authorized, in each fiscal year, to issue framework decrees that allow, among other things, the Treasury to carry out borrowing operations on the domestic or foreign market in the form of short-, medium-, and long-term financial products and instruments, indicating their nominal amount, the interest rate or the criteria for its determination, the duration, the minimum amount that can be subscribed, the placement system, and any other characteristics and methods;

Having regard to Decree No. 101633 of 19 December 2022 (hereinafter the "General Decree") and subsequent amendments and additions, which continuously establish the characteristics and issuance procedures for medium- and long-term government bonds to be placed through auction; Having regard to Ministerial Decree No. 5048315 of 15

December 2023, issued pursuant to Article 3 of the "Consolidated Law" (hereinafter "framework decree"), which defines for the financial year 2024 the objectives, limits and methods to which the Treasury Department must adhere in carrying out the financial operations referred to in the same article, providing that the operations themselves are arranged by the Director General of the Treasury or, by his delegation, by the Director of Directorate II of the same Department and that, in the event of absence or impediment of the latter, the aforementioned operations may be arranged by the same



Director General of the Treasury, even in the presence of continuous delegation; Having

regard to Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012, as subsequently amended by Regulation (EU) No. 2023/2845 of the European Parliament and of the Council of 13 December 2023 as regards the regulation of settlement, the provision of cross-border services, supervisory cooperation, the provision of banking-type ancillary services and the requirements for third-country central securities depositories, and as supplemented by Delegated Regulation (EU) No. 2017/389 of the Commission of 11 November 2016 as regards the parameters for the calculation of financial penalties for settlement fails and the operations of central securities depositories (CSDs) in host Member States and by Commission Delegated Regulation (EU) No. 2018/1229 of 25 May 2018 as regards regulatory technical standards on settlement discipline, as amended by Commission Delegated Regulation (EU) No. 2021/70 of 23 October 2020 with reference to the entry into force thereof, by Commission Delegated Regulation (EU) No. 2022/1930 of 6 July 2022 as regards the date of application of the provisions relating to the buy-in procedure and, lastly, by Commission Delegated Regulation (EU) No. 2023/1626 of the Commission of 19 April 2023 as regards the penalty mechanism for settlement fails relating to cleared transactions that central counterparties submit for settlement purposes;

Having seen Ministerial Decree No. 12953 of 17 February 2023, concerning the "Accounting provisions in the event of delays in the settlement of transactions involving the issuance, exchange and repurchase of government bonds, as well as in repurchase agreements carried out by the Ministry of Economy and Finance"; Having seen Ministerial Decree No. 96718 of 7

December 2012, concerning the "Provisions for the separation, negotiation and reconstitution of the coupon components, the inflation-indexed component and the nominal redemption value of government bonds *(stripping)* "; Having seen Law No. 213 of 30 December 2023, containing the "State budget forecast for the financial year 2024 and the multi-year

budget for the three-year period 2024-2026", and in particular art. 3, paragraph 2, which established the maximum limit for issuing public loans for the same year; Considering that the amount of issues arranged up to September 24, 2024, net of repayments of public loans already made, amounts to 97,284 million euros; Having seen Resolution No.

101204 of November 23, 2023, by which the Director General of the Treasury delegated, effective January 1, 2024, the General Manager Head of Directorate II in relation to the responsibilities

relating to public debt, pursuant to the aforementioned Article 3 of Presidential Decree No. 398/2003, in order to ensure the continuity and timeliness of administrative action;

Having seen its decrees dated 30 July and 28 August 2024, which ordered the issuance of the first four *tranches* of 3.85% multi-year Treasury bonds with accrual date 1 August 2024 and maturity 1 February 2035;

Having deemed it appropriate, in relation to market conditions, to arrange for the issuance of a fifth *tranche* of the aforementioned multi-year Treasury bonds;

Decrees:

Art. 1.

Pursuant to and for the purposes of Article 3 of the "Consolidated Law" and the "Framework Decree", the issuance of a fifth *tranche* of 3.85% multi-year Treasury bonds is hereby ordered, with accrual beginning August 1, 2024, and maturing February 1, 2035. The issuance of the aforementioned *tranche* is ordered for a nominal amount ranging from a minimum of 3,000 million euros to a maximum of 3,500 million euros.

The bonds bear gross annual interest of 3.85%, payable in two semi-annual installments in arrears, on February 1st and August 1st of each year of the loan term. The first semi-annual installment is payable on February 1st, 2025, and the last on February 1st, 2035.

On the same bonds, operations can be carried out to separate and reconstitute the coupon components from the redemption value of the security *("coupon stripping").*

The characteristics and methods of issuing the aforementioned securities are those defined in the "general decree", which is hereby deemed to be fully referred to and to which reference is made for anything not expressly provided for in this decree.

Art. 2.

Operators' bids for the *tranche* referred to in Article 1 of this decree must be received by 11:00 a.m. on September 27, 2024, in compliance with the procedures set forth in Articles 7, 8, 9, 10, and 11 of the "General Decree."

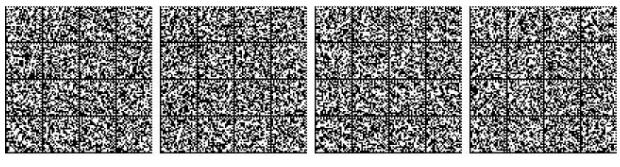
The placement commission, equal to 0.200% of the subscribed nominal capital, will be paid according to the methods set out in Article 8 of the "General Decree" indicated in the preamble.

Art. 3.

At the end of the allocation operations referred to in the previous article, the placement of the sixth *tranche* of the securities themselves takes place, according to the methods indicated in articles 12, 13, 14 and 15 of the "general decree".

The amount of the *tranche* relating to the security subject to this issue will be equal to 20 percent as established by Article 14, paragraph 2, of the "General Decree".

Government bond specialists have the right to participate in the supplementary placement by submitting subscription applications by 3.30 pm on 30 September 2024.



Art. 4.

Settlement of the bonds subscribed at auction and in the supplementary placement will be carried out by the assigned operators on October 1, 2024, at the auction price and with the payment of gross interest for sixty-one days. To this end, the Bank of Italy will automatically enter the related items into the clearing and settlement service with a value date equal to the settlement date.

In the event of delay in the settlement of the securities referred to in this decree, the provisions of Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 and Ministerial Decree No. 12953 of 17 February 2023, cited in the preamble, shall apply.

Art. 5.

On 1 October 2024, the Bank of Italy will pay the proceeds of the bonds assigned at the auction hammer price, together with the gross annual interest rate of 3.85%, due to the State, to the Rome Section of the State Treasury.

The aforementioned Treasury section issues, for said payments, separate receipts of income to the State budget, with the amount relating to the proceeds of the issue being charged to Chapter X, Chapter 5100, Article 3 (parliamentary voting units 4.1.171) and to Chapter 3240, Article 3 (parliamentary voting units 2.1.93) for the amount relating to the gross interest due.

Art. 6.

The interest charges relating to the financial years 2025 to 2035, as well as the charge for the repayment of the capital relating to the financial year 2035, will be charged to the chapters that will be entered in the expenditure forecast of the Ministry of Economy and Finance for those years and corresponding, respectively, to chapters 2214 (parliamentary voting units 21.1) and 9502 (parliamentary voting units 21.2) of the budget forecast for the current year.

The amount of the placement commission, provided for in art. 2 of this decree, will be recorded, at each quarterly payment interval, by the Treasury sections among the "payments to be settled" and will be charged to chapter 2247 (parliamentary voting unit 21.1; management code 109) of the expenditure forecast of the Ministry of Economy and Finance for the financial year 2024 or the corresponding year for subsequent years.

This decree will be published in the *Official Journal* of the Italian Republic.

Rome, September 27, 2024

p. The Director General of the Treasury: IACOVONI

24A05139

DECREES AND RESOLUTIONS OF OTHER AUTHORITIES

INTERMINISTERIAL COMMITTEE FOR ECONOMIC PLANNING AND SUSTAINABLE DEVELOPMENT

RESOLUTION 9 July 2024·

Public Investment Evaluation and Verification Units. Allocation of resources for 2024 (Article 1, paragraph 7, of Law No. 144/1999). (Resolution No. 50/2024).

THE INTERMINISTERIAL COMMITTEE
FOR ECONOMIC PLANNING
AND SUSTAINABLE DEVELOPMENT

IN THE SESSION OF 9 JULY 2024

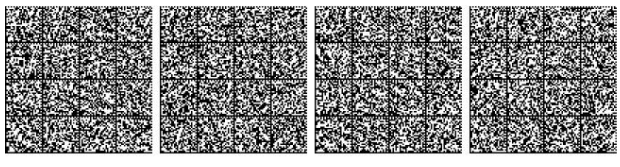
Having regard to Law No. 48 of 27 February 1967, concerning the "Powers and Organization of the Ministry of Budget and Economic Planning and the Establishment of the Committee of Ministers for Economic Planning" and, in particular, Article 16, concerning the establishment and powers of the Interministerial Committee for Economic Planning, hereinafter CIPE, as well as subsequent legislative provisions relating to the Committee,

and in particular Legislative Decree No. 111 of 14 October 2019, containing "Urgent measures to comply with the obligations set out in Directive 2008/50/EC on air quality and extension of the deadline referred to in Article 48, paragraphs 11 and 13, of Legislative Decree No. 189 of 17 October 2016, converted, with amendments, by Law No. 229 of 15 December 2016", which in Article 1 *-bis* inserted in the conversion law No. 12 December 2019. 141, has established that from 1 January 2021, in order to "strengthen the coordination of public policies with a view to pursuing the sustainable development objectives indicated" by the UN 2030 Agenda, the CIPE will assume "the name of Interministerial Committee for Economic Planning and Sustainable Development", hereinafter CIPESS, and that "starting from the same date, in Law 27 February 1967, no. 48, and in any other current provision, any reference" to the CIPE "must be understood as referring to"

CIPESS;

Having seen Law No. 400 of 23 August 1988, concerning "Regulation of Government Activity and Organization of the Presidency of the Council of Ministers", and subsequent amendments, and in particular, Article 5, paragraph 2;

Having seen the decree of the President of the Council of Ministers of 1 October 2012, and subsequent amendments, containing



"Organization of the general structures of the Presidency of the Council of Ministers", and, in particular, Article 20, relating to the organization and tasks of the Department for Economic Policy Planning and Coordination, hereinafter DIPE;

Having regard to Law No. 144 of 17 May 1999, containing "Measures regarding investments, delegation to the Government for the reorganization of employment incentives and the legislation governing INAIL, as well as provisions for the reorganization of social security institutions", and subsequent amendments, in particular Article 1, paragraph 7, which provides for the establishment of a Fund to be distributed, hereinafter the Fund, following a resolution of this Committee, after consulting the Permanent Conference for Relations between the State, the Regions and the Autonomous Provinces of Trento and Bolzano, hereinafter the CSR, aimed at co-financing the activities of the Public Investment Evaluation and Verification Units within central and regional administrations, hereinafter the Units, including horizontal functions, represented by the coordination role of this Committee and the public investment monitoring system, hereinafter the MIP, established within this Committee;

Having regard to Article 145, paragraph 10, of Law No. 388 of 23 December 2000, containing "Provisions for the preparation of the annual and multi-year State budget" (2001 Finance Law), pursuant to which the resources allocated to the aforementioned Fund may co-finance, among other things, the launch of the MIP System and expenses related to the operation of the network of Units and the coordination role played by this Committee;

Having seen Article 11 of Law No. 3 of 16 January 2003, containing "Regulatory provisions on public administration", and subsequent amendments, which establishes that, for the purposes of the MIP, each new public investment project must be provided with a Single Project Code, hereinafter CUP;

Having seen Article 2, paragraph 109, of Law No. 191 of 23 December 2009, containing "Provisions for the preparation of the annual and multi-year State budget" (2010 Finance Law), pursuant to which the Nuclei of the Autonomous Provinces of Trento and Bolzano are excluded from the distribution, by virtue of the contribution of these provinces to the rebalancing of public finances as provided for by Article 79 of Presidential Decree No. 670 of 31 August 1972 (Special Statute for Trentino-Alto Adige);

Having regard to Law No. 136 of 13 August 2010, containing the "Extraordinary Plan against the Mafia, as well as delegation to the Government regarding anti-Mafia legislation" and subsequent amendments, and in particular Articles 3 and 6 concerning the use of the CUP to ensure the traceability of financial flows aimed at preventing criminal infiltration, and the penalty for failure to use it, respectively;

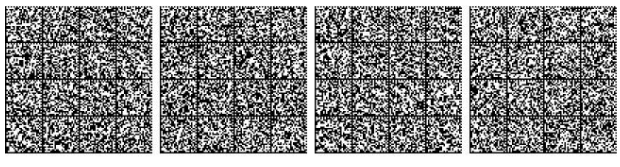
Having seen Legislative Decree No. 228 of 29 December 2011, concerning the "Implementation of Article 30, paragraph 9, letters *a) , b) , c)* and *d) ,* of Law No. 196 of 31 December 2009, regarding the evaluation of investments relating to public works", and in particular Article 7, paragraph 1, which provides that the Ministries shall identify the bodies responsible for evaluation activities within the Units;

Having seen Legislative Decree No. 229 of 29 December 2011, concerning the "Implementation of Article 30, paragraph 9, letters *e) , f)* and *g)* of Law No. 196 of 31 December 2009, regarding monitoring the progress of public works, verifying the use of funding within the expected timeframe and establishing the Works Fund and the Projects Fund", and in particular Article 1, paragraph 1, letter *d) ,* which requires that within the information systems indicated in the aforementioned article: "the work must be accompanied, for the purposes of obtaining the relevant public funding, by the Single Project Code (CUP) which must appear already in the presentation phase and in all subsequent transactions, also pursuant to Law No. 136 of 13 August 2010. The Tender Identification Code cannot be issued by the authority for the supervision of public contracts for works, services and supplies for contracts aimed at the implementation of public investment projects which do not have the mandatory Single Project Code pursuant to Article 136. 11 of Law 16 January 2003, n. 3, and subsequent amendments.»

Having regard to the Prime Ministerial Decree of 21 December 2012, no. 262, provided for by Article 7, paragraph 3, of the aforementioned Legislative Decree no. 228 of 2011, containing "Regulations for units established within central State administrations with the function of ensuring technical support for the planning, evaluation and monitoring of public interventions"; Having regard to Article 41, paragraph 2, of Legislative Decree no.

76 of 16 July 2020, containing "Urgent measures for simplification and digital innovation", converted, with amendments, by Law no. 120 of 11 September 2020, which amended Article 1, paragraph 7, of the aforementioned Law no. 144, providing, from 2021, the annual allocation of 900,000 euros for the operation of the MIP/CUP system;

Having regard to art. 50, paragraph 10, of Legislative Decree no. 13 of 24 February 2023, containing "Urgent provisions for the implementation of the National Recovery and Resilience Plan (NRRP) and the National Plan of Investments complementary to the NRRP (PNC), as well as for the implementation of cohesion policies and the common agricultural policy", converted, with amendments, by Law no. 41 of 21 April 2023, which provides for: "reorganization, without new or greater burdens on public finances, of the Evaluation and Analysis Unit for Programming (NUVAP) referred to in art. 1, paragraph 2, of the Prime Ministerial Decree no. 300 of 29 December 2014, published in the *Official Journal* of the Italian Republic, which is renamed



“Cohesion Policy Unit (NUPC)” and to which the functions and activities assigned by the current provisions to the Verification and Control Unit referred to in art. 1, paragraph 3, of the Decree of the President of the Council of Ministers of 19 November 2014, published in the *Official Journal* of the Italian Republic - no. 300 of 29 December 2014 are transferred”»;

Having seen the decree of the President of the Council of Ministers of 13 December 2023, approving the budget forecast of the Presidency of the Council of Ministers for the year 2024, with which €2,811,210.00 was allocated to the Fund;

Considering that also for 2024 the coordination activities entrusted to the Department for Planning and Coordination of Economic Policy of the Presidency of the Council of Ministers, hereinafter DIPE, will be carried out without burdening the aforementioned Fund;

Having seen CIPE resolution no. 26 of 18 March 2013, and in particular point 6, which states that "The Units will submit an annual report, to be prepared by 31 January of each year, on the activities carried out and the expenditure incurred using both CIPE allocations and co-financing from the administrations to which they belong";

Having seen CIPE resolution no. 126 of 22 December 2017, which established that the DIPE would establish a permanent committee to ensure multilevel governance and ongoing monitoring of the Fund's availability and the continuity and adequacy of financial flows;

Having seen note no. 3396 of 10 July 2017, with which the DIPE forwarded the proposal to revise the criteria for allocating resources earmarked for co-financing the operating costs of the Units to the CSR, for the purpose of expressing its competent opinion;

Whereas the CSR, with opinion no. 114 of 27 July 2017, approved the aforementioned proposal;

Considering that the DIPE has periodically convened the aforementioned Permanent Table, the last annual meeting of which was held on 16 April 2024;

Having seen DIPE note no. 5164 of 22 May 2024, with which the DIPE forwarded to the CSR the proposed distribution of the Fund intended for the co-financing of the operating expenses of the evaluation and verification units of public investments of central and regional administrations for the 2024 financial year;

Whereas in its meeting of 14 June 2024, the CSR expressed a favorable opinion with opinion no. 91/CSR regarding the aforementioned proposal for the distribution of the Fund intended for the co-financing of the operating costs of the evaluation and verification units for public investments of central and regional administrations for the 2024 financial year;

Having seen the decree of the President of the Republic of 31 October 2022, with which Senator Alessandro Morelli was appointed Undersecretary of State to the Presidency of the Council of Ministers;

Having seen the decree of the President of the Council of Ministers of 25 November 2022, by which Senator Alessandro Morelli was appointed secretary of the Interministerial Committee for Economic Planning and Sustainable Development (CIPESS), and assigned to him, among other things, the delegation to exercise the functions pertaining to the President of the Council of Ministers regarding the coordination of economic policy and the planning and monitoring of public investments, including those aimed at pursuing sustainable development, as well as those under public-private partnerships;

Having seen the note from the office of the USS Undersecretary dated 19 June 2024, no. 327, purchased with DIPE Prot. no. 6358 of 20 June 2024, with which the secretary of the CI-PESS proposes the inclusion on the agenda of this Committee of the proposal for the distribution of the Fund intended for the co-financing of the operating expenses of the evaluation and verification units of public investments of central and regional administrations for the year 2024;

Taking into account the examination of the proposal which is the subject of this resolution carried out pursuant to the internal regulations of this Committee, approved by resolution no. 82 of 28 November 2018, containing the "Internal Regulations of the Interministerial Committee for Economic Planning" as amended by resolution no. 79 of 15 December 2020, containing the "Internal Regulations of the Interministerial Committee for Economic Planning and Sustainable Development (CIPESS)";

Having seen note no. 7106 of 9 July 2024, prepared jointly by the DIPE and the Ministry of Economy and Finance, which forms the basis of today's Committee meeting, containing the preliminary assessments regarding this resolution;

Having regard to the debate which took place during today's meeting of the Committee;

On the proposal of the secretary of this Committee;

Resolution:

1. The distribution for the year 2024 of the Fund referred to in Article 1, paragraph 7, of Law No. 144 of 17 May 1999 is approved, according to the scheme shown in Table 1 below:

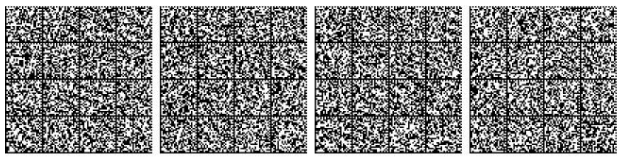
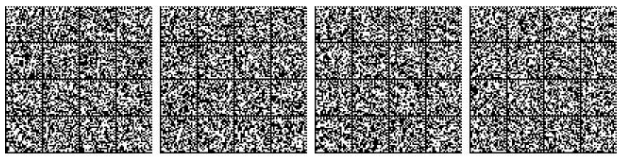


Table 1 - Proposed distribution of the Fund - Year 2024

(Law No. 144/1999, Article 1, Paragraph 7)

Section 1 - Regions	
Abruzzo	66,783.39
Basilicata	75,759.61
Calabria	87,515.34
Campania	139,875.84
Emilia-Romagna	93,784.27
Friuli Venezia Giulia	62,980.65
Lazio	106,635.23
Liguria	69,570.58
Lombardy	108,879.21
Marche	46,040.28
Molise	39,157.40
Piedmont	92,685.66
Puglia	112,536.33
Sardinia	81,969.75
Sicily	135,144.89
Tuscany	85,674.08
Umbria	58,863.36
Aosta Valley	53,774.46
Veneto	100,630.93
Total	**1,618,261.27**



Section 2 - Central Administrations	
Agricultural policies	36,618.59
Justice	36,618.59
Culture	36,618.59
MIT	36,618.59
Health	36,618.59
Internal	36,618.59
PCM-DIPE	36,618.59
Total	**256,330.14**
Section 3 - Horizontal functions	
MIP/CUP	900,000.00
PCM-NUPC (formerly NUVAP)	36,618.59
Total	**936,618.59**
Total Fund Year 2024	**2.811.210,00**

The Vice President: GIORGETTI

The Secretary: MORELLI

Registered at the Court of Auditors on 17 September 2024
Office for the Control of the Acts of the Ministry of Economy and Finance, No. 1249

24A05073

EXTRACTS, SUMMARIES AND PRESS RELEASES

ITALIAN MEDICINES AGENCY

Marketing authorization for the medicinal product for human use, based on dorzolamide hydrochloride and timolol maleate, «Dorzolamide Timolol Omnivision».

Extract from AAM/ AIC resolution no. 204 of September 12, 2024

European Procedure No. AT/H/1213/001/DC. The marketing authorization for the medicinal product DOR-ZOLAMIDE/TIMOLOL OMNIVISION, the characteristics of which are summarized in the Summary of Product Characteristics (SmPC), Package Leaflet (PL), and Labels (Eti), which are integral parts of the decision referred to in this extract, is hereby granted in the pharmaceutical forms, dosages, and packaging under the conditions and with the specifications indicated below.

AIC Holder: OmniVision Italia Srl, with registered office and domicile tax office in - via Montefeltro n. 6 - 20156 Milan, Italy.

Packaging:

«20 mg/mL + 5 mg/mL eye drops, solution» 1 5 mL HDPE container with dropper pump - AIC n. 051124016 (in base 10) 1JS5TJ (in base 32);

«20 mg/mL + 5 mg/mL eye drops, solution» 1 9 mL HDPE container with dropper pump - AIC n. 051124028 (in base 10) 1JS5TW (in base 32);

«20 mg/mL + 5 mg/mL eye drops, solution» 2 HDPE containers of 9 mL with dropper pump - AIC n. 051124030 (in base 10) 1JS5TY (in base 32).

Active ingredients: dorzolamide hydrochloride and timolol maleate.

Manufacturer responsible for batch release:

Tubilux Pharma Spa - via Costarica n. 20/22 - 00071, Pomezia (Rome).

Classification for reimbursement purposes

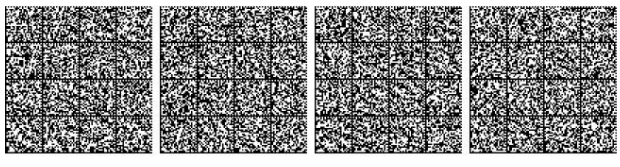
The following classification is adopted for the above mentioned packages: for reimbursement purposes:

Classification for reimbursement purposes: specific section of the class referred to in Article 8, paragraph 10, letter *c)* of Law No. 537 of 24 December 1993 and subsequent amendments, dedicated to drugs not yet evaluated for reimbursement purposes, called class C(nn).

Classification for supply purposes

For the above packages, the following classification is adopted for supply purposes:

classification for supply purposes: RR: medicinal product subject to medical prescription.



Printed

The medicinal product packages must be placed on the market with labels and information leaflets compliant with the text attached to the resolution referred to in this extract.

The summary of product characteristics attached to the resolution, referred to in this extract, is approved.

Pursuant to Article 80, paragraphs 1 and 3 of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the labeling must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Market protection

The MAH for a generic drug is solely responsible for full compliance with the terms set forth in Article 10, paragraphs 2 and 4, of Legislative Decree No. 219 of 24 April 2006, as subsequently amended and supplemented. This provision stipulates that a generic drug may not be placed on the market until ten years have elapsed from the initial authorization of the reference drug, or until eleven years have elapsed from the initial authorization of the reference drug, if, during the first eight years of that decade, the MAH has obtained authorization for one or more new therapeutic indications that, following the scientific evaluation prior to authorization, have been deemed to provide a significant clinical benefit compared to existing therapies.

This paragraph and the provisions contained therein are to be considered applicable only where the described situation occurs.

Patent protection

The holder of the MA for the generic drug is exclusively responsible for ensuring full compliance with the industrial property rights relating to the reference medicinal product and with the current regulatory provisions on patent matters.

The MAH is also responsible for full compliance with the provisions of Article 14, paragraph 2 of Legislative Decree No. 219 of 24 April 2006, and subsequent amendments and additions, pursuant to which those parts of the summary of product characteristics of the reference medicinal product that refer to indications or dosages still covered by patent at the time the medicinal product is placed on the market are not included in the printed materials.

This paragraph and the provisions contained therein are to be considered applicable only where the described situation occurs.

Periodic Safety Update Reports (PSURs)

The marketing authorisation holder shall submit periodic safety update reports for this medicinal product in accordance with the requirements set out in the list of Union reference dates (EURD list) referred to in Article 107 *-qua-*

, paragraph 7) of Directive 2010/84/EC and published on the web portal *of* the European Medicines Agency.

Conditions or limitations regarding the safe and effective use of the medicinal product

The marketing authorisation holder is required to implement the pharmacovigilance activities and actions required and detailed in the Risk Management Plan (RMP).

Validity of the authorization

The authorisation is valid until the European Common Renewal Date (CRD) 15 March 2029, as indicated in the end-of-procedure (EoP) notification sent by the Reference Member State (RMS).

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05011

Marketing authorization for the medicinal product for human use, based on cyclopentolate hydrochloride, «Ple-gik».

Extract from AAM/ AIC resolution no. 214/2024 of 18 September 2024

The marketing of the medicinal product PLEGIK, the characteristics of which are summarised in the summary of product characteristics (SmPC), package leaflet (PL) and labels (Eti), integral parts of the determination referred to in this extract, is authorised in the pharmaceutical form, dosage and packaging under the conditions and with the specifications indicated below.

AIC Holder: Medivis Srl, with registered office and tax domicile in via Carnazza, 34/C - 95030 Tremestieri Etneo - Catania, Italy.

Packaging: «10 mg/ml eye drops, solution» 1 5 ml LDPE bottle with dropper.

AIC n. 049916012 (base 10) 1HMB3D (base 32).

Active ingredient: cyclopentolate hydrochloride.

Manufacturers responsible for batch release:

Laboratorio Edol - Produtos Farmacèuticos, SA, Av. 25 de Abril, 6-6a, 2795-225 Linda-a-Velha, Portugal; Laboratorio Edol -

Produtos Farmacèuticos, SA, Rua Quinta Do Salrego N 22-22a, Portela De Carnaxide, Carnaxide, 2790-144 - Rua Casal Do Canas 6-6a, Carnaxide, 2790-204, Portugal.

Classification for reimbursement purposes

Packaging AIC n. 049916012 «10 mg/ml eye drops, solution» 1 5 ml LDPE bottle with dropper.

Classification for reimbursement purposes: specific section of the class referred to in art. 8, paragraph 10, letter *c) ,* of Law no. 537 of 24 December 1993 and subsequent amendments, dedicated to drugs not yet evaluated for reimbursement purposes, called class C(nn).

Classification for supply purposes

Packaging: AIC n. 049916012 «10 mg/ml eye drops, solution» 1 5 ml LDPE bottle with dropper.

Classification for supply purposes: RR - medicinal product subject to medical prescription.

Printed

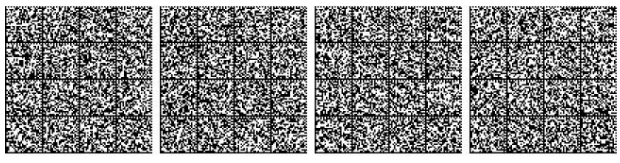
The medicinal product packaging must be marketed with labels and package inserts compliant with the text attached to the resolution, referred to in this extract. The summary of product

characteristics attached to the resolution, referred to in this extract, is approved.

Pursuant to Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the labeling must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Market protection

The holder of the marketing authorization for the generic drug is exclusively responsible for full compliance with the terms set out in Article 10, paragraphs 2 and 4, of Legislative Decree No. 219 of 24 April 2006, and subsequent amendments and additions, according to which a generic drug cannot be placed on the market until ten years have elapsed from the initial authorization of the reference drug, or until eleven years have elapsed from the initial authorization of the reference drug.



if during the first eight years of that decade, the MAH has obtained an authorization for one or more new therapeutic indications which, from the scientific evaluation preliminary to the authorization, have been deemed to provide a significant clinical benefit compared to existing therapies.

This paragraph and the provisions contained therein are to be considered applicable only where the described situation occurs.

Patent protection

The holder of the MA for the generic drug is exclusively responsible for ensuring full compliance with the industrial property rights relating to the reference medicinal product and with the current regulatory provisions on patent matters.

The MAH is also responsible for full compliance with the provisions of Article 14, paragraph 2, of Legislative Decree No. 219 of 24 April 2006, and subsequent amendments and additions, pursuant to which those parts of the summary of product characteristics of the reference medicinal product that refer to indications or dosages still covered by patent at the time the medicinal product is placed on the market are not included in the printed materials.

This paragraph and the provisions contained therein are to be considered applicable only where the described situation occurs.

Periodic Safety Update Reports (PSURs)

The marketing authorisation holder shall submit periodic safety update reports for this medicinal product in accordance with the requirements set out in the list of Union reference dates (EURD list) referred to in Article 107 *-qua-*

third, par. 7), of Directive 2010/84/EC and published on the *web* portal of the European Medicines Agency.

Conditions or limitations regarding the safe and effective use of the medicine

The marketing authorisation holder is required to implement the pharmacovigilance activities and actions required and detailed in the Risk Management Plan (RMP).

Validity of the authorization

The authorization is valid for five years from the date of effectiveness of this resolution.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05012

Amendment to the marketing authorisation for the medicinal product for human use, based on clotrimazole, «Clozol».

Extract from AAM/ PPA resolution no. 714/2024 of 13 September 2024

Transfer of ownership: AIN/2024/1395. The transfer

of ownership of the marketing authorization for the medicinal product listed below is authorized. The medicinal product, currently registered in the name of FG Srl, with registered office and tax domicile at Via San Rocco, 6, 85033 Episcopia, Potenza, Italy, and tax code 01444240764, is authorized.

Medicine: CLOZOL.

Packaging: «2% vaginal cream» 1 30 g aluminum tube with 6 disposable applicators.

AIC n. 049989015, to the

company Farmitalia Industria chimica farmaceutica Srl with registered office and tax domicile at Via Pinciana, 25, 00198 Rome, tax code 03115090874.

Printed

The marketing authorisation holder of the above-mentioned medicinal product must make the necessary changes to the summary of product characteristics from the date of entry into force of the resolution referred to in this extract; to the information leaflet and labels from the first production batch following the entry into force of the resolution referred to in this extract.

Stock disposal

Batches of the medicinal product, already produced and released in the name of the previous owner on the date of entry into force of the determination referred to in this extract, may be kept on the market until the expiry date indicated on the label.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05014

Amendment of the marketing authorization of the medicinal product for human use, based on meropenem, «Merrem».

Extract from AAM/ PPA resolution no. 717/2024 of June 13, 2024

The marketing authorisation is amended, following the variation approved by the reference Member State (France): Type II - CI4) Amendment of paragraphs 4.4, 4.8 and 5.1 of

the summary of the product characteristics and paragraph 4 of the package leaflet,

relating to the medicinal product MERREM in the pharmaceutical form, dosage and packaging indicated below:

pack «500 mg powder for solution for injection for intravenous use» 10 vials - AIC n. 028949081;

pack «1000 mg powder for solution for injection for use intravenous» 10 vials - AIC n. 028949093.

Practice code: VC2/2023/520.

Procedure number: FR/H/0467/001-002/II/042.

Owner: Pfizer Italia Srl, with registered office and tax domicile in Via Isonzo n. 71 - 04100 Latina, tax code 06954380157.

The corrected and approved forms are attached to the resolution referred to in this extract.

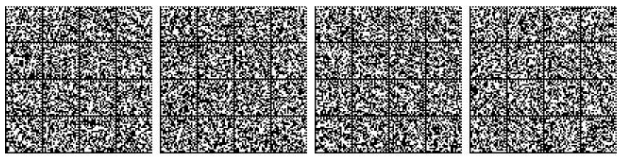
Printed

1. The marketing authorization holder must make the authorized changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract; and to the package leaflet no later than six months after the same date.

2. In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to avail itself of the complementary use of foreign languages must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic and batches produced during the period referred to in the previous paragraph of this extract, which do not contain the authorized changes, may remain on the market until the expiration date of the medicinal product indicated on the label. Starting thirty days after the date of publication of this extract in the *Official Journal* of the Italian Republic, pharmacists are required to provide the updated package leaflet to users, who choose to collect it in paper or analog format, or through alternative digital methods. The MAH shall make the updated package leaflet accessible to the pharmacist within the same deadline.



Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05015

Amendment to the marketing authorisation for the medicinal product for human use, based on dextromethorphan hydrobromide, «Vicks Cough Sedative».

Extract from AAM/ PPA resolution no. 713/2024 of 13 September 2024

The following variation is authorised: type II -

CI4). Paragraph 5.1 of the summary of product characteristics is amended for the medicinal product VICKS COUGH SEDATIVO in the pharmaceutical form, dosage and pack sizes listed below:

AIC No. 028688012 - "1.33 mg/ml syrup" 120 ml bottle; AIC No. 028688024 -

"1.33 mg/ml syrup" 180 ml bottle. Furthermore, according to the list of standard

terms of the European Pharmacopoeia, the modification of the name of the already authorized packages as indicated below is approved:

from: AIC n. 028688012 - «1.33 mg/ml syrup» 120 ml bottle
ml;

a: AIC n. 028688012 - «1.33 mg/ml syrup» 1 120 ml glass bottle with child-resistant closure;

from: AIC n. 028688024 - «1.33 mg/ml syrup» 180 ml bottle
ml;

a: AIC n. 028688024 - «1.33 mg/ml syrup» 1 180 ml glass bottle with child-resistant closure.

Practice code: VN2/2024/94.

AIC Holder: Procter & Gamble Srl, with registered office and tax domicile in Viale Giorgio Ribotta, 11 - 00144 Rome, tax code 05858891004.

The corrected and approved forms are attached to the resolution referred to in this extract.

Printed

1. The marketing authorization holder must make the authorized changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract.

2. In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to avail itself of the complementary use of foreign languages must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic, and batches produced during the period referred to in the previous paragraph of this extract, may be kept on the market until the expiry date of the medicinal product indicated on the label, pursuant to art. 1, paragraph 7, of AIFA resolution no. DG/821/2018 of 24 May 2018, published in the *Official Journal* of the Italian Republic no. 133 of 11 June 2018.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05016

Amendment to the marketing authorisation for the medicinal product for human use, based on the dry extract of black cohosh (Cicifuga recamosa (L.) Nutt., rhizoma, «Cimifemin».

Extract from AAM/ PPA resolution no. 746/2024 of September 20, 2024

Transfer of ownership: AIN/2024/1352. The transfer of

ownership of the marketing authorization for the medicinal product listed below, currently registered in the name of Yes Pharmaceutical Development Services GmbH, with registered office at Basler Strasse, 7 - 61352 - Bad Homburg, Germany, is authorized.

Medicine: CIMIFEMIN.

Packaging:

049810017 - «2.5 mg tablets» 20 tablets in PVC blister/
PVDC/AL;

049810029 - «2.5 mg tablets» 60 tablets in PVC/AL blister
PVDC/AL;

049810031- «2.5 mg tablets» 100 tablets in PVC/AL blister
PVDC/AL, to

the company Schaper & Brummer GmbH & Co. Kg, with registered office in Bahnhofstrasse, 35, 38259 - Salzgitter, Germany.

Printed

The marketing authorization holder for the above-mentioned medicinal product must make the necessary changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract; to the package leaflet and to the labels from the first production batch following the entry into force of the decision referred to in this extract.

Stock disposal

Batches of the medicinal product, already produced and released in the name of the previous owner on the date of entry into force of the determination referred to in this extract, may be kept on the market until the expiry date indicated on the label.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05033

Amendment to the marketing authorisation for the medicinal product for human use, based on [18F]PSMA-1007, «Radelumin».

Extract from AAM/ PPA resolution no. 739/2024 of September 20, 2024

The marketing authorisation is amended, following the following variations, approved by the Reference Member State (RMS), with procedure FR/H/0797/II/005/G, relating to the medicinal product RADELUMIN:

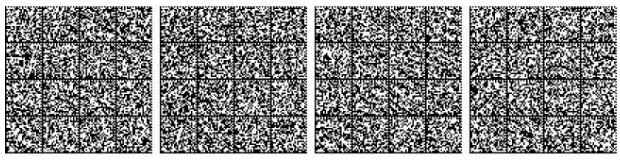
Type IA $_{IN}$, B.II.b.2 - changes in the importer, batch release procedures and quality control testing of the finished product; *c)* replacement or addition of a manufacturer responsible for importing and/or releasing batches; 2. including batch control/testing:

Synektik Pharma Sp z oo, Szaserów Street 128, 04-141, Warsaw, Poland, as responsible for batch release of the finished product; B.II.b.1 - replacement or addition of

Type IA $_{IN}$, a manufacturing site for part or all of the manufacturing process of the finished product; *a)* secondary packaging site;

Type II, B.II.b.1 - replacement or addition of a manufacturing site for part or all of the manufacturing process of the finished product; *c)* site where all manufacturing operations are carried out, with the exception of batch release, batch control and secondary packaging, or intended for pharmaceutical forms produced by complex manufacturing processes;

Type II, BIa1 - change in the manufacturer of a raw material, reagent or intermediate product used in the manufacturing process



manufacturing of an active substance or change in the manufacturer of the active substance (including, where applicable, quality control sites), for which a certificate of conformity to the European Pharmacopoeia is not available; (g) introduction of a new manufacturer of the active substance who does not have the support of an ASMF and who requires a significant update of the relevant section of the active substance dossier.

The printed materials, paragraph 6 of the package leaflet, are modified. as described: 6.

Package contents and other information

[...]

Producers:

[...]

Synektik Pharma Sp. z oo ul. Szaserów 128, 04-141, Warszawa, Poland.

The marketing authorisation is amended, following the following variations, approved by the Reference Member State (RMS), with procedure FR/H/0797/II/011/G, relating to the medicinal product RADELUMIN:

Type IA, n. 2 variations, B.II.b.2 - changes in the importer, in the batch release procedures and in the quality control tests of the finished product; *a)* replacement or addition of a site where batch control/testing is carried out; Type IA

IN, B.II.b.2 - changes at importer level, of mo-
batch release and quality control testing of the finished product; *(c)* replacement or addition of a manufacturer responsible for the import and/or release of batches; 2. including batch control/testing:

Synektik Pharma Sp. z oo, Artwiÿskiego Street 3, 25-734 Kielce, Poland, as responsible for batch release of the finished product; B.II.b.1 - replacement or

Type IA IN, addition of a manufacturing site for part or all of the manufacturing process of the finished product; *a)* secondary packaging site;

Type II, B.II.b.1 - replacement or addition of a manufacturing site for part or all of the manufacturing process of the finished product; *c)* site where all manufacturing operations are carried out, with the exception of batch release, batch control and secondary packaging, or intended for pharmaceutical forms produced by complex manufacturing processes;

Type II, BIa1 - change in the manufacturer of a starting material, reagent or intermediate used in the manufacturing process of an active substance or change in the manufacturer of the active substance (including, where applicable, quality control sites), for which a certificate of conformity to the European Pharmacopoeia is not available; (g) introduction of a new manufacturer of the active substance who does not have the support of an ASMF and who requires a significant update of the relevant section of the active substance dossier.

The printed material, paragraph 6 of the package leaflet, is amended. as described:

6. Package contents and other information

[...]

Producers:

[...]

Synektik Pharma Sp. z oo ul. Artwiÿskiego 3, 25-734 Kielce, Poland.

Packaging and AIC numbers:

050594011 - «1300 mbq/ml solution for injection» 1 vial 10 ml glass multidose containing from 0.3 ml to 10 ml;

050594023 - «1300 mbq/ml solution for injection» 1 vial 15 ml glass multidose containing from 0.3 ml to 15 ml;

050594035 - «1300 mbq/ml solution for injection» 1 vial 20 ml glass multidose containing from 0.3 ml to 20 ml.

MA holder: ABX advanced biochemical compounds - Biome-dizinische Forschungsreagenzien GmbH, with registered office and tax domicile in Heinrich-Gläser-Straße 10-14, 01454 Radeberg, Germany.

European procedures: FR/H/0797/II/005/G - FR/H/0797/II/011/G.

Practice codes: VC2/2023/241 - VC2/2023/289.

Printed

The marketing authorisation holder must make the authorised changes from the date of entry into force of the determination, referred to in this extract, to the summary of product characteristics; within and no later than six months from the same date to the package leaflet.

In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the above must notify AI-FA in advance and provide a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic and batches produced during the period referred to in the previous paragraph of this extract, which do not contain the authorised modifications, may be kept on the market until the expiry date of the medicinal product indicated on the label, pursuant to art. 1, paragraph 7 of AIFA resolution no. DG/821/2018 of 24 May 2018, published in the *Official Journal* no. 133 of 11 June 2018.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05053

Amendment to the marketing authorisation for the medicinal product for human use, based on [18F]PSMA-1007, «Radelumin».

Extract from AAM/ PPA resolution no. 741/2024 of September 20, 2024

The marketing authorisation is amended, following the following variations, approved by the Reference Member State (RMS), with procedure FR/H/0797/II/013/G, relating to the medicinal product RADELUMIN:

type IA IN, B.II.b.2 - changes in the importer, batch release procedures and quality control testing of the finished product; *c)* replacement or addition of a manufacturer responsible for importing and/or releasing batches; 2. including batch control/testing:

Seibersdorf Labor GmbH, 2444 Seibersdorf, Austria; type AI

IN, B.II.b.1 - replacement or addition of a manufacturing site for part or all of the manufacturing process of the finished product; *a)* secondary packaging site;

type II, B.II.b.1 - replacement or addition of a manufacturing site for part or all of the manufacturing process of the finished product; *c)* site where all manufacturing operations are carried out, with the exception of batch release, batch control and secondary packaging, or intended for pharmaceutical forms produced by complex manufacturing processes;

Type II, BIa1 - change in the manufacturer of a starting material, reagent or intermediate used in the manufacturing process of an active substance or change in the manufacturer of the active substance (including, where applicable, quality control sites), for which there is no certificate of conformity with the European Pharmacopoeia; *g)* introduction of a new manufacturer of the active substance who does not have the support of an ASMF and who requires a significant update of the relevant section of the active substance dossier; Type IA, B.II.b.2 - changes in the importer, batch release procedures and quality control testing of the finished product; *a)* replacement or

addition of a site where batch control/testing is carried out.

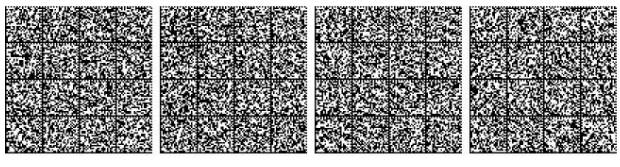
The printed material, paragraph 6 of the package leaflet, is amended. as described:

6. Package contents and other information

[…]

Producers:

[…]



Seibersdorf Labor GmbH, 2444 Seibersdorf, Austria.

The marketing authorisation is amended, following the following variations, approved by the Reference Member State (RMS), with procedure FR/H/0797/II/018/G, relating to the medicinal product RADELUMIN:

Type II, BIa1 - change in the manufacturer of a starting material, reagent or intermediate used in the manufacturing process of an active substance or change in the manufacturer of the active substance (including, where applicable, quality control sites), for which a certificate of conformity to the European Pharmacopoeia is not available; *g)* introduction of a new manufacturer of the active substance who is not supported by an ASMF and who requires a significant update of the relevant section of the active substance dossier; B.II.b.2 - changes in the importer, batch release procedures and quality control testing of the finished product; *c)* replacement or addition of a manufacturer responsible

type IA $_{IN}$, for import and/or batch release; 2. including batch control/testing:

Advanced Accelerator Applications Molecular Imaging Fran-ce SAS Saint Cloud, 3 rue Charles Lauer, 92210 Saint-Cloud, France; B.II.b.1 - replacement or

type IA $_{IN}$, addition of a manufacturing site for part or all of the manufacturing process of the finished product; *a)* secondary packaging site.

type II, B.II.b.1 - replacement or addition of a manufacturing site for part or all of the manufacturing process of the finished product; *c)* site where all manufacturing operations are carried out, with the exception of batch release, batch control and secondary packaging, or intended for pharmaceutical forms produced using complex manufacturing processes.

The printed material, paragraph 6 of the package leaflet, is amended. as described:

6. Package contents and other information

[…]

Producers:

[…]

AAA Molecular Imaging France SAS Saint Cloud, 3 Rue Charles Lauer, 92210 Saint-Cloud, France.

AIC packs n.:

050594047 - «2000 mbq/ml solution for injection» 1 vial no 10 ml glass multidose containing from 0.3 ml to 10 ml;

050594050 - «2000 mbq/ml solution for injection» 1 vial no 15 ml glass multidose containing from 0.3 ml to 15 ml;

050594062 - «2000 mbq/ml solution for injection» 1 vial no 20 ml glass multidose containing from 0.3 ml to 20 ml.

MA holder: ABX advanced biochemical compounds - Bio-medizinische Forschungsreagenzien GmbH, with registered office and tax domicile in Heinrich-Gläser-Straße 10-14, 01454 Radeberg, Germany.

European procedures: FR/H/0797/II/013/G - FR/H/0797/II/018/G.

Practice codes: VC2/2023/306 - VC2/2023/455.

Printed

The medicinal product packages must be placed on the market with the printed materials previously authorized by this administration, with only the modifications necessary to comply with this resolution.

The marketing authorization holder must make the authorized changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract; and to the package leaflet no later than six months after the same date.

In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the above must notify AI-FA in advance and provide a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic and batches produced during the period referred to in the previous paragraph of this extract, which do not contain the authorized modifications, may be kept on the market until the expiry date of the medicinal product indicated on the label, pursuant to art. 1, paragraph 7 of AIFA resolution no. DG/821/2018 of 24 May 2018, published in the *Official Journal* of the Italian Republic no. 133 of 11 June 2018.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05054

Amendment of the marketing authorization

of the medicinal product for human use, based on folic acid, «Acido folico Aristo».

Extract from AAM/PPA resolution no. 742/2024 of September 20, 2024

The marketing of the medicinal product ACIDO is authorised FOLIC ARISTO, also in the pharmaceutical form, dosage and packaging indicated below:

packaging: «5 mg tablets» 84 tablets in PVC blister/PVDC/PVC/Al - AIC n. 048957070 (base 10) 1GQ1NG (base 32).

Active ingredient: folic acid.

Marketing Authorisation Holder: Aristo Pharma GmbH, with registered office and domicile tax office at Wallenroder Straße 8-10, 13435 Berlin, Germany.

European procedure: DE/H/8095/001/IA/005.

Practice code: C1A/2024/1737.

Classification for reimbursement purposes

For the new packaging mentioned above, the following classification is adopted for reimbursement purposes: C(nn).

Classification for supply purposes

For the new packaging mentioned above, the following classification is adopted for supply purposes: RR (medicines subject to medical prescription).

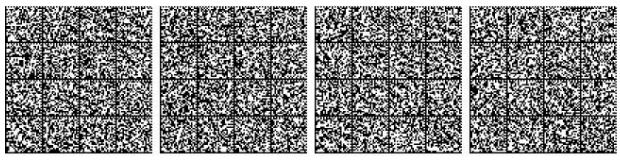
Printed

The medicinal product packages must be placed on the market with the printed materials previously authorized by this administration, with only the modifications necessary to comply with this resolution.

Pursuant to Article 80, paragraphs 1 and 3 of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the labeling must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05055



Amendment to the marketing authorisation for the medicinal product for human use, based on itraconazole, «Itragerm».

Extract from AAM/ PPA resolution no. 743/2024 of September 20, 2024

The marketing authorisation is amended, following the following variation, approved by the Reference Member State (RMS), relating to the medicinal product ITRAGERM:

Type II, CI2b) - Update of the printed information based on clinical studies, with the addition of information regarding "gastric acidity"; paragraphs 4.4, 4.5, 5.2 of the summary of product characteristics and the corresponding paragraphs of the package leaflet are modified.

AIC packs n.:

044757019 - «50 mg hard capsules» 4 capsules in PVC/Pe/ blister Pvdc/Al (Triplex);

044757021 - «50 mg hard capsules» 6 capsules in PVC/Pe/ blister Pvdc/Al (Triplex);

044757033 - «50 mg hard capsules» 7 capsules in PVC/Pe/ blister Pvdc/Al (Triplex);

044757045 - «50 mg hard capsules» 8 capsules in PVC/Pe/ blister Pvdc/Al (Triplex);

044757058 - «50 mg hard capsules» 14 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757060 - «50 mg hard capsules» 15 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757072 - «50 mg hard capsules» 18 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757084 - «50 mg hard capsules» 28 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757096 - «50 mg hard capsules» 30 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757108 - «50 mg hard capsules» 60 capsules in PVC blister/ Pe/Pvdc/Al (Triplex);

044757110 - «50 mg hard capsules» 4 capsules in blister Opa/ Al/Pvc;

044757122 - «50 mg hard capsules» 6 capsules in blister Opa/ Al/Pvc;

044757134 - «50 mg hard capsules» 7 capsules in blister Opa/ Al/Pvc;

044757146 - «50 mg hard capsules» 8 capsules in blister Opa/ Al/Pvc;

044757159 - «50 mg hard capsules» 14 capsules in blister Opa/ Al/Pvc;

044757161 - «50 mg hard capsules» 15 capsules in blister Opa/ Al/Pvc;

044757173 - «50 mg hard capsules» 18 capsules in blister Opa/ Al/Pvc;

044757185 - «50 mg hard capsules» 28 capsules in blister Opa/ Al/Pvc;

044757197 - «50 mg hard capsules» 30 capsules in blister Opa/ Al/Pvc;

044757209 - «50 mg hard capsules» 60 capsules in blister Opa/ Al/Pvc;

044757211 - «50 mg hard capsules» 15 capsules in HDPE bottle; 044757223 - «50 mg hard capsules» 30 capsules in HDPE bottle; 044757235 - «50 mg hard capsules» 60 capsules in HDPE bottle; 044757247 - «50 mg hard capsules» 90 capsules in HDPE bottle.

The corrected and approved forms are attached to the resolution referred to in this extract.

AIC Holder: Isdin Srl, tax code 06115640960, with registered office registered office and tax domicile at Via Statuto n. 4, 20121 Milan, Italy.

European procedure: ES/H/0599/001/II/027.

Practice code: VC2/2023/600.

Printed

The marketing authorisation holder must make the authorised changes from the date of entry into force of the determination, referred to in this extract, to the summary of product characteristics; within and no later than six months from the same date to the package leaflet.

In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to use foreign languages in addition to the above must notify AI-FA in advance and provide a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic and batches produced during the period referred to in the previous paragraph of this extract, which do not contain the authorized changes, may remain on the market until the expiration date of the medicinal product indicated on the label. Starting thirty days after the date of publication of this extract in the *Official Journal* of the Italian Republic, pharmacists are required to provide the updated package leaflet to users, who choose to collect it in paper or analog format, or through alternative digital methods. The MAH shall make the updated package leaflet accessible to the pharmacist within the same deadline.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05056

Amendment to the marketing authorisation for the medicinal product for human use, based on cytisinicline «Ko-bayzaren».

Extract from AAM/ PPA resolution no. 744/2024 of September 20, 2024

Transfer of ownership: AIN/2024/1477.

Name change: N1B/2024/1017. The

transfer of ownership of the marketing authorization for the medicinal product listed below is authorized. The medicinal product, currently registered to Alfrapharma Srl, with registered office and tax domicile at Viale Manzoni, 59 - 00185 Rome, tax code 07227261000, is authorized.

Medicine: KOBAYZAREN.

Packaging: «1.5 mg film-coated tablets» 100 tablets in PVC/PVDC/AL blister - AIC n. 049451014.

To Adamed Srl, with registered office and tax domicile at Via Giuseppe Mazzini, 20 - 20123 Milan, tax code 10753240968.

With change of name of the medicine to RECIGAR.

Printed

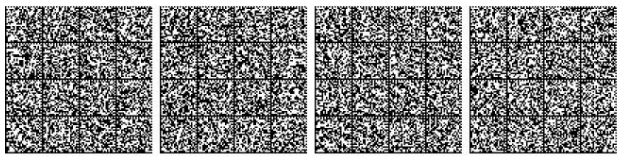
The marketing authorization holder for the above-mentioned medicinal product must make the necessary changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract; to the package leaflet and to the labels from the first production batch following the entry into force of the decision referred to in this extract.

Stock disposal

Batches of the medicinal product, already produced and released in the name of the previous owner on the date of entry into force of the determination referred to in this extract, may be kept on the market until the expiry date indicated on the label.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05057



Amendment to the marketing authorization for the medicinal product for human use, based on Tiapride hydrochloride, «Italprid».

Extract from AAM/ PPA resolution no. 752/2024 of September 20, 2024

The following change is authorized.

Type II - CI3.b) paragraphs 4.3, 4.4, 4.5, 4.6, 4.8, 4.9, 5.3 of the summary of product characteristics are amended.

Editorial and QRD compliance changes in sections 4.7, 5.1, 6.5, 6.6 and 8 of the summary of product characteristics and changes to sections 2, 3 and 4 of the package leaflet.

The labels have also been updated in accordance with the QRD *template* and the national requirements for the *Blue Box* have been updated . ·

Regarding the medicinal product ITALPRID in the pharmaceutical form, dosage and packaging indicated below: AIC n. 023913015

- 20 tablets 100 mg.

Practice code: VN2/2022/201.

AIC Holder: Teofarma Srl with registered office and tax domicile at Via Fratelli Cervi, 8 - 27010 Valle Salimbene, Pavia, tax code 01423300183.

The corrected and approved forms are attached to the resolution referred to in this extract.

Printed

1. The marketing authorization holder must make the authorized changes to the summary of product characteristics from the date of entry into force of the decision referred to in this extract; and to the package leaflet and labeling no later than six months after the same date.

2. In compliance with Article 80, paragraphs 1 and 3, of Legislative Decree No. 219 of April 24, 2006, and subsequent amendments and additions, the package leaflet and labels must be written in Italian and, limited to medicinal products marketed in the Province of Bolzano, also in German. The MAH intending to avail itself of the complementary use of foreign languages must notify AIFA in advance and maintain a certified translation of the texts in German and/or another foreign language. Failure to comply with the provisions on labeling and the package leaflet will result in the penalties set forth in Article 82 of the aforementioned Legislative Decree.

Stock disposal

Both batches already produced on the date of publication of this extract in the *Official Journal* of the Italian Republic and batches produced during the period referred to in the previous paragraph of this extract, which do not contain the authorized changes, may remain on the market until the expiration date of the medicinal product indicated on the label. Starting thirty days after the date of publication of this extract in the *Official Journal* of the Italian Republic, pharmacists are required to provide the updated package leaflet to users, who choose to collect it in paper or analog format, or through alternative digital methods. The MAH shall make the updated package leaflet accessible to the pharmacist within the same deadline.

Effective date of the resolution: from the day following its publication, in extract, in the *Official Journal* of the Italian Republic.

24A05058

Revocation, upon surrender, of the marketing authorization for certain medicinal products for human use

With resolution no. aRM - 179/2024 - 1214 of 18 September 2024, pursuant to art. 38, paragraph 9, of Legislative Decree no. 219/2006, upon renunciation by Weleda Italia Srl, the marketing authorization for the following homeopathic medicinal products, in the indicated packages, was revoked:

medicine: ZINNOBER;

packaging: 045807043;

Description: «D6 tablets» 1 glass bottle of 180 tablets; packaging: 045807031; Description:

«D6 tablets» 1 glass bottle of

80 tablets; packaging: 045807029; Description: «D20 tablets» 1 glass bottle of 180 tablets;

packaging: 045807017;

Description: «D20 tablets» 1 glass bottle of 80 tablets; Medicine: CONCHAE;

Packaging: 047360019;

Description: «D30 oral powder» 1 glass bottle of 20 g; Medicine: BRYONIA;

packaging: 046134045;

description: «6 DH oral drops, solution» 1 50 ml glass dropper bottle;

packaging: 046134033;

description: «6 DH oral drops, solution» 1 20 ml glass dropper bottle;

packaging: 046134021;

description: «3 DH oral drops, solution» 1 50 ml glass dropper bottle;

Packaging: 046134019;

Description: «3 DH oral drops, solution» 1 20 ml glass dropper bottle.

If there are stocks of the recalled medicines in the distribution channel that are still valid, they may be disposed of within one hundred and eighty days of the date of publication of this resolution.

24A05059

Revocation, upon renouncement, of the authorization for the parallel import of the medicinal product for human use «Ananase».

By means of aRM - 180/2024 - 3912 determination of 19 September 2024, the import authorisation for the packages of medicinal products for human use listed below, issued under the parallel import authorisation procedure, was revoked, following the waiver by Pricetag Spa.

Medicine: PINEAPPLE:

Packaging: 045081015;

Description: «40 mg coated tablets» 20 coated tablets.

Country of origin: Portugal.

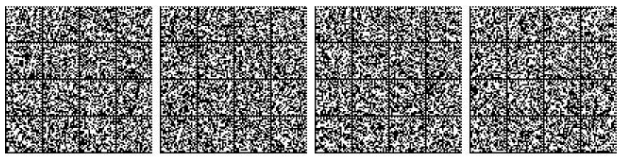
If there are stocks of the revoked medicine in the distribution channel that are still valid, they may be disposed of within one hundred and eighty days of the date of publication of this resolution.

24A05060

MINISTRY OF AGRICULTURE, OF FOOD SOVEREIGNTY AND OF THE FORESTS

Application procedures and content for registration of grapevine varieties and clones in the National Register. Repeal of the decree of September 30, 2021.

Ministerial Decree No. 316697 of July 16, 2024, containing the submission procedures and content of the application for registration of grapevine varieties and clones in the National Register, pursuant to Articles 13 and 17 of Legislative Decree No. 16 of February 2, 2021. Repeal of Ministerial Decree No. 489243 of September 30, 2021, has been published on the website of the Ministry of Agriculture, Food Sovereignty and Forestry, at https://www.politicheagricole.it/flex/cm/pages/ServeBLOB.



php/L/IT/IDPagina/22019 and on the website of the National Plant Protection Service at the web page https://www.protezionedellepiante.it/decreto-ministeriale-del-16-luglio-2024-n-0316697-modalita-di-presentazione-e-contenuti-della-domanda-di-iscrizione-di-varieta-e-cloni-di-vite-al-registro-nazionale-di-cui-agli-artt-13-e-17-del-d/

24A05074

MINISTRY OF THE ENVIRONMENT AND ENERGY SECURITY

Call for expressions of interest for the preparation of opinions on the verification of the economic and financial capacity of operators in the energy and/or mining sectors and for their positioning for the purposes of issuing and managing licenses and authorizations granted in the aforementioned sectors.

Please be advised that the Directorate General for Energy Sources and Qualifications of the Ministry of the Environment and Energy Security, on September 23, 2024, approved the exploratory call for expressions of interest from qualified entities to prepare opinions on the verification of the economic-financial capacity (CTE) of operators in the energy and/or mining sector and for their relative positioning for the purposes of issuing and managing the qualifications and authorizations granted in the aforementioned sector.

The full invitation to express interest, as reported above, is published on the Ministry's website (https://unmig.mase.gov.it/).

24A05075

MINISTRY OF BUSINESS AND MADE IN ITALY

Distribution of the residual resources available pursuant to Article 6, paragraph 2, of the decree of 3 June 2024, for the recognition, for the year 2024, of the contribution for the installation of new LPG or methane systems for motor traction on approved category M1 vehicles.

By decree of the Director General for Industrial Policy, Reconversion and Industrial Crisis, Innovation, SMEs and Made in Italy of September 23, 2024, the resources referred to in Article 4, paragraph 1, of the Directorial Decree of June 3, 2024, were allocated, reserving a portion equal to 30% (thirty percent) for grants for the installation of new methane fuel systems and a portion equal to 70% (seventy percent) for grants for the installation of new LPG fuel systems.

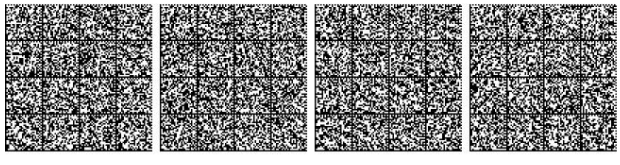
The decree was issued pursuant to Article 6, paragraph 2, of the Directorial Decree of June 3, 2024, based on monitoring of the measure as of September 15, 2024.

Pursuant to Article 32 of Law No. 69 of June 18, 2009, the full text of the Directorial Decree is published and available for consultation on the website of the Ministry of Business and Made in Italy at https://www.mimit.gov.it

24A05100

MARGHERITA CARDONA ALBINI, *editor* DELIA CHIARA, *deputy editor*

(WI-GU- 2024 -GU1- 230) Rome, 2024 - State Mint and Polygraphic Institute SpA



TERMS OF SALE

The "Official Gazette" and all other publications of the Institute are on sale to the public:

— at the Institute's sales point in Piazza G. Verdi, 1 - 00198 Rome 06-8549866☎— at the concessionary bookshops listed on the websites www.ipzs.it and www.gazzettaufficiale.it

The Institute holds the Gazettes for the last four years for sale until they are exhausted. Mailing requests may be sent to:

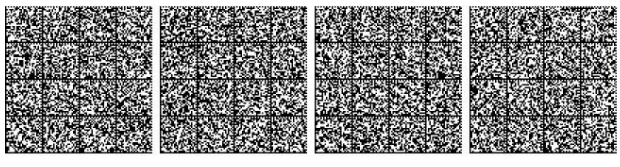
State Printing Office and Mint SpA
Official Gazette Sales Via Salaria,

691 00138 Rome fax:
06-8508-3466 e-

mail:

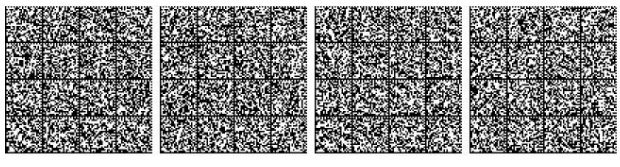
informazioni@gazzettaufficiale.it

Please ensure that, in addition to the requested Official Gazette (GU) file, the shipping and billing addresses (if different) are specified in the order, as well as the tax information (tax code and VAT number, if applicable) required by Legislative Decree 223/2007. The cost of the order, plus a shipping fee, will be paid in cash upon receipt.



white

blank page blank page blank page page



OFFICIAL JOURNAL
OF THE ITALIAN REPUBLIC

SUBSCRIPTION FEES (subject to adjustment) valid from 1 JANUARY 2024

OFFICIAL JOURNAL – PART I (legislative)

SUBSCRIPTION FEE

Type A Subscription to the General Series issues, including all ordinary supplements:		
*(including shipping costs €257.04)**	- annual **€**	**438.00**
*(including shipping costs €128.52) **	- half-yearly **€**	**239.00**
Type B Subscription to the issues of the 1st Special Series for the proceedings before the Constitutional Court: *(including shipping costs €19.29)**		
*(including shipping costs €9.64)**	- annual **€** - half-yearly **€**	**68.00** **43.00**
Type C Subscription to the issues of the 2nd Special Series for EU documents: *(including shipping costs €41.27)** *(including shipping costs €20.63)**	- annual **€** - half-yearly **€**	**168.00** **91.00**
Type D Subscription to the issues of the 3rd Special Series dedicated to regional laws and regulations: - annual **€** - half-yearly **€**		
*(including shipping costs €15.31)**		**65.00**
*(including shipping costs €7.65)**		**40.00**
Type E Subscription to the issues of the 4th special series intended for the competitions announced from the State and other public administrations: *(of which shipping costs €50.02)** *(of which shipping costs €25.01)**	- annual **€** - half-yearly **€**	**167.00** **90.00**
Type F Subscription to the issues of the General Series, including all ordinary supplements, and to the issues of the four special series: *(including shipping costs €383.93*)* *(including shipping costs €191.46)**	- annual **€** - half-yearly **€**	**819.00** **431.00**

NB: The subscription to GURI type A and F includes the monthly indexes

BOOKLET PRICES (plus shipping costs)

Sales prices: general series special	€	1.00
series (excluding competitions), every 16 pages or fraction special	€	1.00
series issue, *competitions,* single price supplements	€	1.50
(ordinary and extraordinary), every 16 pages or fraction	€	1.00

4% VAT paid by the Publisher

OFFICIAL JOURNAL - PART II

*(including shipping costs €40.05)**	- annual **€**	**86.72**
*(including shipping costs €20.95)**	- half-yearly **€**	**55.46**

Selling price for one issue, every 16 pages or fraction thereof (plus shipping costs) €1.01 (€0.83+VAT)

A 22% VAT rate is applied to publications in Part II. Please note that pursuant to Law 190 of 23 December 2014, Article 1, paragraph 629, the state entities specified therein are required to pay the Institute only the taxable portion relating to the subscription fee. For further information, please contact editoria@ipzs.it.

OFFICIAL COLLECTION OF REGULATORY DOCUMENTS Annual

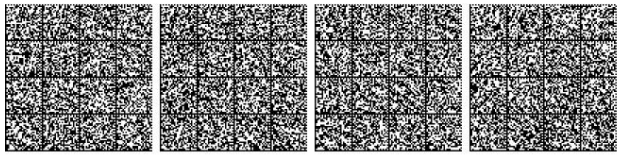
subscription Annual	€	**190.00**
subscription for regions, provinces and municipalities – 5% DISCOUNT Separate	€	**180.50**
volume (plus shipping costs)	€	6.00 pm

4% VAT paid by the Publisher

For international publications, the price of subscriptions and separate issues, including back issues, including ordinary and special supplements, is doubled. For domestic publications, the price of separate issues, including ordinary and special supplements, including those for previous years, is doubled. For entire years, the current subscription price is doubled.
Shipping costs for requests for individual issues to be sent by mail are determined from time to time based on the number of copies requested.
Any undelivered issues may be provided free of charge within 60 days of the issue's publication date. After this period, they will only be provided for a fee.

NB – The shipment of the issues will begin within 15 days of activation by the Official Journal Subscriptions Office.
THE COMMERCIAL DISCOUNTS APPLIED REMAIN CONFIRMED TO THE **COSTS ONLY** FROM **SUBSCRIPTION**

* postal rates pursuant to Law 27 February 2004, n. 46 (GU n. 48/2004) for subjects registered with the ROC



€1.00

45-410100241001