EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

Italy

Legislative Decree of 18 May 2018, no. 65, Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 promulgating measures for a high common level of security of network and information systems across the Union.

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Italy

Legislative Decree of 18 May 2018, no. 65, Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 promulgating measures for a high common level of security of network and information systems across the Union.

(18G00092) (GU General Series no. 132 of 09-06-2018)

THE PRESIDENT OF THE REPUBLIC

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

Having regard to the Law of 24 December 2012, no. 234, promulgating general rules on Italy's participation in the training and implementation of European Union legislation and policies;

Having regard to the Law of 25 October 2017, no. 163, delegating powers to the Government for the transposition of European directives and the implementation of other European Union acts - European Delegation Law 2016-2017;

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

Having regard to 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;

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/GAI;

Having regard to the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;

Having regard to Commission Implementing Regulation no. 2018/151/EU of 30 January 2018 promulgating detailed rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council regarding the further specification of the elements that digital service providers must take into consideration for the purposes of managing the risks posed to the security of networks and information systems and the parameters for determining the significant impact of an incident, if any;

Having regard to the Decree Law of 27 July 2005, no. 144, converted with modifications by the Law of 31 July 2005, no. 155, promulgating measures to combat international terrorism;

Having regard to the Legislative Decree of 4 March 2014, no. 39, implementing Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, replacing the 2004 Framework Decision;

Having regard to the Law of 3 August 2007, no. 124, promulgating an information system for the security of the Republic and new rules on secrecy;

Having regard to the Decree-Law of 30 October 2015, no. 174, converted with modifications by the Law of 11 December 2015, no. 198, promulgating the extension of the international missions of the Armed Forces and the police, development cooperation initiatives and support for the reconstruction processes and participation in the initiatives of international organisations for the consolidation of peace and stabilisation processes;

Having regard to the Decree Law of 22 June 2012, no. 83, converted with modifications, by the Law of 7 August 2012, no. 134, promulgating urgent measures for the growth of the country, and, in particular, Article 19, establishing the Agency for Digital Italy (AgID);

Having regard to the Legislative Decree of 7 March 2005, no. 82, promulgating the digital administration code and, in particular, provisions on AgID functions and IT security;

Having regard to the Legislative Decree of 11 April 2011, no. 61, implementing Directive 2008/114/EC, promulgating the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;

Having regard to the regulation adopted by Decree of the President of the Council of Ministers of 6 November 2015, no. 5, promulgating provisions for the administrative protection of state secrets and classified information and exclusive dissemination;

Having regard to the Directive adopted by the Decree of the President of the Council of Ministers of 17 February 2017, promulgating guidelines for national cyber protection and IT security, published in Official Gazette no. 87 of 13 April 2017;

Having regard to the Legislative Decree of 30 June 2003, no. 196, promulgating the code on the protection of personal data;

Having regard to Legislative Decree of 1 August 2003, no. 259, promulgating the code on electronic communications;

Having regard to the Legislative Decree of 23 June 2011, no. 118, promulgating provisions on the harmonisation of the accounting systems and budget formats of the Regions, local authorities and their bodies, pursuant to Articles 1 and 2 of the Law of 5 May 2009, no. 42;

Having regard to the Preliminary Resolution of the Council of Ministers, adopted at the meeting of 8 February 2018;

Having obtained the opinion of the Unified Conference referred to in Article 8 of the Legislative Decree of 28 August 1997, no. 281, given in the session of 19 April 2018;

Having obtained the opinions of the competent Commissions of the Chamber of Deputies and of the Senate of the Republic;
Having regard to the Resolution of the Council of Ministers, adopted at the meeting of 16 May 2018;

Upon the proposal of the President of the Council of Ministers and the Minister of Economic Development, in agreement with the Ministers of Foreign Affairs and International Cooperation, Justice, Interior, Defence, Health and Economy and Finance;

Hereby issues
the following Legislative Decree:

Chapter I

General Provisions

Art. 1

Object and scope of application

1. This Decree establishes measures aimed at achieving a high level of security of the network and information systems at the national level, helping to increase the common level of security in the European Union.

2. For the purposes of paragraph 1, this Decree provides for:
a) the inclusion in the national cyber security strategy of provisions on the security of networks and information systems falling within the scope of application of this Decree;
b) the designation of the competent national authorities and the single point of contact, as well as the Computer Security Incident Response Team (CSIRT) at the national level for the performance of the tasks referred to in Annex I;
c) the compliance with obligations by operators of essential services and digital service providers in relation to the adoption of security measures and notification of incidents with a significant impact;
d) the national participation in the European cooperation group, with a view to collaboration and exchange of information between the Member States of the European Union, as well as increasing the trust between them;
e) the national participation in the CSIRT network with a view to ensuring rapid and effective technical-operational cooperation.

3. The provisions on security measures and notification of incidents referred to in this Decree do not apply to companies subject to the obligations referred to in Articles 16a and 16b of the Legislative Decree of 1 August 2003, no. 259, nor to trust service providers subject to the obligations referred to in Article 19 of Regulation (EU) no. 910/2014.

4. This Decree applies without prejudice to the provisions of the Legislative Decree of 11 April 2011, no. 61, of Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/GAI.

5. Without prejudice to the provisions of Article 346 of the Treaty on the Functioning of the European Union, confidential information, in accordance with the provisions of European Union and national legislation, in particular with regard to business confidentiality, shall be exchanged with the European Commission and other NIS competent authorities only to the extent that such an exchange is necessary for the purposes of the application of this Decree. The information exchanged is relevant and commensurate with the purpose. The exchange of information protects its confidentiality and protects the security and commercial interests of operators of essential services and digital service providers.

6. This Decree is without prejudice to the measures adopted to safeguard the essential functions of the State, in particular for the protection of national security, including measures to protect information, in cases where disclosure is deemed contrary to the essential interests of security and maintenance of public order, in particular for the purposes of investigation, detection and the prosecution of crimes.

7. Where the obligations imposed on operators of essential services or digital service providers to ensure the security of their networks and information systems or to notify incidents are the subject of a specific legal act of the European Union, the provisions of that legal act are applied to the extent that the effects of such obligations are at least equivalent to those of the obligations referred to in this

Decree.

Art. 2

Processing of personal data

1. The processing of personal data in application of this Decree is carried out in accordance with the Legislative Decree of 30 June 2003, no. 196, as amended.

Art. 3

Definitions

1. For the purposes of this Decree, the following definitions are given:
a) the competent NIS authority, the authority competent by sector, in matters of network and information system security, referred to in Article 7, paragraph 1;
b) the CSIRT, Computer Security Incident Response Team, referred to in Article 8;
c) a single point of contact, the body responsible at the national level for coordinating matters relating to the security of networks and information systems and cross-border cooperation at EU level;
d) law enforcement authorities, the central body of the Ministry of the Interior for the security and the supervision of telecommunication services, referred to in Article 7a of the Decree-Law of 27 July 2005, no. 144, converted with modifications by the Law of 31 July 2005, no. 155;
e) a network and information system being:
1) an electronic communication network pursuant to Article 1, paragraph 1, letter dd), of the Legislative Decree of 1 August 2003, no. 259;
2) any device or group of interconnected or connected 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;
f) the security of the network and information systems, the ability of a network and information systems to resist, at a certain level of confidentiality, any action that compromises the availability, authenticity, integrity or confidentiality of the data stored or transmitted or processed and the related services offered or accessible through this network or information systems;
g) an operator of essential services, public or private entity, of the type referred to in Annex II, which meets the criteria referred to in Article 4, paragraph 2;
h) digital service, a service within the meaning of Article 1, paragraph 1, letter 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) a digital service provider, any legal person providing a digital service;
l) an incident, any event with a real detrimental effect on the security of the network and information systems;
m) the handling of the incident, all the 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 potentially detrimental effects for the security of the network and information systems;
o) a 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, which the competent NIS authority or the National CSIRT may contact in place of the digital services provider, as regards the latter's obligations under this Decree;
p) a rule, a rule pursuant to Article 2, first paragraph, number 1), of Regulation (EU) no. 1025/2012;
q) a specification, a technical specification pursuant to Article 2, first paragraph, number 4), of Regulation (EU) no. 1025/2012;
r) an internet interchange point (IXP), a network infrastructure that allows the interconnection of more

than two independent autonomous systems, mainly in order to facilitate the exchange of internet traffic; an IXP provides interconnection only to autonomous systems; an IXP does not require internet traffic passing between any pair of participating autonomous systems to pass through a third autonomous system, nor does it alter or otherwise interfere with such traffic;
s) the domain name system (DNS), is a distributed and hierarchical naming system in a network that forwards requests for domain names;
t) a DNS service provider, an entity that provides DNS services on the internet;
u) a registry of top level domain names, an entity that administers and registers internet domain names within a specific top level domain (TLD);
v) an online market, a digital service that allows consumers or professionals, as defined respectively in Article 141, paragraph 1, letters a) and b), of the Legislative Decree of 6 September 2005, no. 206, to conclude sales or online service contracts with professionals both on the website of the online marketplace and on the website of a professional who uses the IT services provided by the online market;
z) an online search engine, a digital service that allows the user to search, in principle, all websites or on websites in a particular language based on 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 may be found;
aa) cloud computing service, a digital service that allows access to a scalable and elastic set of shareable IT resources.

Art. 4

Identification of essential service operators

1. By 9 November 2018, with their own provisions, the competent NIS authorities shall identify for each sector and subsector referred to in Annex II, the operators of essential services with an office within the national territory. The operators that provide health assistance activities 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. The operators that supply and distribute water intended for human consumption are identified by Decree of the Minister for the Environment and for the Protection of the Territory and the 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 operators of essential services are as follows:
a) an entity provides a service that is essential for the maintenance of fundamental social and/or economic activities;
b) the provision of this service relies upon the network and information systems;
c) an incident would have a material adverse effect on the provision of that service.

3. In addition to the criteria indicated in paragraph 2, when identifying operators of essential services, the documents produced in this regard by the Cooperation Group referred to in Article 10 are taken into account.

4. For the purposes of paragraph 1, before the adoption of the measures provided for by the same provision, if an entity provides a service referred to in paragraph 2, letter a) on the national territory and in another or other Member States of the European Union, the competent NIS shall consult the competent authorities of the other Member States.

5. A national list of essential service operators has been established at the Ministry of Economic Development.

6. The list of essential service operators identified pursuant to paragraph 1 is reviewed in the same manner as referred to in paragraph 1 and, if necessary, updated on a regular basis, and at least every two years after 9 May 2018, by the competent NIS authorities and is communicated to the Ministry of Economic Development.

7. By 9 November 2018, and every two years thereafter, the single contact point 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 essential services.

8. The information referred to in paragraph 7 shall include at least:
a) national measures enabling 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 significance in relation to that sector;
d) the thresholds, if any, to determine the relevant level of supply with reference to the number of users that rely upon this service referred to in Article 5, paragraph 1, letter a), or on the significance of that particular operator of essential services referred to in Article 5, paragraph 1, letter f).

Art. 5

Relevant negative effects

1. For the purpose of determining the significance of the negative effects referred to in Article 4, paragraph 2, letter c), the competent NIS authorities shall consider the following cross-sectoral factors:
a) the number of users that rely upon the service provided by the entity involved;
b) the dependence of other sectors listed in Annex II on the service provided by that entity;
c) the impact that incidents may have, in terms of extent and duration, on economic and social activities or on public safety;
d) the market share of said entity;
e) the geographical spread in relation to the area that could be affected by an incident;
f) the significance of the entity in maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of this service.

2. In order to determine the significant negative effects of an incident, sectoral factors are also considered, where appropriate.

Chapter II

Strategic and institutional context

Art. 6

National Cyber Security Strategy

1. The President of the Council of Ministers shall adopt, after consulting the Interministerial Committee for the Security of the Republic (CISR), the national cyber security strategy for the protection of the security of networks and systems of national interest.

2. As part of the national cyber security strategy, the following are indicated in particular for the security of networks and information systems falling within the scope of application of this Decree:
a) the objectives and priorities regarding the security of networks and information systems;
b) the framework of governance to achieve the objectives and priorities, including the roles and responsibilities of public bodies and other relevant actors;
c) measures on preparedness, response and recovery, including collaboration between the public and private sectors;
d) programs for the training, awareness and education relating to the security strategy of networks and information systems;
e) research and development plans;

f) a risk assessment plan;
g) the list of the various actors involved in the implementation.

3. With the procedure referred to in paragraph 1, guidelines shall be adopted for the implementation of the national cyber security strategy.

4. The Presidency of the Council of Ministers shall convey the national cyber security strategy to the European Commission within three months of its adoption. The conveyance of elements of the strategy relating to national security may be excluded.

Art. 7

Competent national authorities and single point of contact

1. The following are designated as the Competent NIS Authorities for the sectors and subsectors listed in Annex II and for the services listed in Annex III:
a) the Ministry of Economic Development for the energy sector, electricity, gas and oil subsectors and for the digital infrastructure sector, and the IXP, DNS, TLD as well as digital services subsectors;
b) the Ministry of Infrastructure and Transport for the transport sector, air, rail, water and road subsectors;
c) the Ministry of Economy and Finance for the banking sector and for the infrastructure sector of the financial markets, in collaboration with the supervisory authorities of the sector, the Bank of Italy and Consob, in accordance with the established methods of collaboration and exchange of information by Decree of the Minister of Economy and Finance;
d) the Ministry of Health for the health care activities, as defined by Article 3, paragraph 1, letter a), of the Legislative Decree of 4 March 2014, no. 38, provided by operators employed or appointed by that Ministry or affiliated with it and the Regions and Autonomous Provinces of Trento and Bolzano, directly or through the territorially competent health authorities, for health care activities provided by operators authorised and accredited by the Regions or autonomous Provinces in the territorial areas of their respective competence;
e) the Ministry of the Environment and the Protection of the Territory and the Sea and the Regions and Autonomous Provinces of Trento and Bolzano, directly or through the territorially competent Authorities, with regard to the supply and distribution of drinking water.

2. The competent NIS Authorities are responsible for the implementation of this Decree with regard to the sectors referred to in Annex II and the services referred to in Annex III and supervise the application of this Decree at the national level, also exercising the relative powers of inspection and sanctions.

3. The Department of Information Security (DIS) is designated as the single point of contact for the security of networks and information systems.

4. The single point of contact performs a liaison function to ensure the cross-border cooperation of the competent NIS authorities with the competent authorities of the other Member States, as well as with the cooperation group referred to in Article 10 and the CSIRT network referred to Article 11.

5. The single point of contact collaborates in the cooperation group effectively, efficiently and securely with the representatives designated by the other states.

6. The competent NIS authorities and the single point of contact shall consult, in accordance with current legislation, the law enforcement authority and the Guarantor for the protection of personal data and collaborate with them.

7. The Presidency of the Council of Ministers shall promptly communicate to the European Commission the designation of the single point of contact and that of the competent NIS authorities, the related tasks and any subsequent changes. Appropriate forms of publicity are assured for the designations.

8. The expenses deriving from this Article, equal to 1,300,000 euros starting from 2018, shall be provided pursuant to Article 22.

Art. 8

Computer Security Incident Response Team - CSIRT

1. The Italian CSIRT is established by the Presidency of the Council of Ministers and carries out the tasks and functions of the national Computer Emergency Response Team (CERT), referred to in Article 16a of the Legislative Decree of 1 August 2003, no. 259, and of the CERT-PA, already operating at the Agency for Digital Italy pursuant to Article 51 of the Legislative Decree of 7 March 2005, no. 82.

2. The organisation and functioning of the Italian CSIRT are governed by a Decree of the President of the Council of Ministers pursuant to Article 7 of the Legislative Decree of 30 July 1999, no. 303, to be adopted by 9 November 2018. For the performance of the functions of the Italian CSIRT, the Presidency of the Council of Ministers makes use of a maximum contingent of thirty personnel, of which fifteen are chosen from among employees of other public administrations, in leadership or out of office, for which Article 17, paragraph 14, of the law of 15 May 1997, no. 127 applies, and fifteen are to be hired, within the limit of the current human resources cap, in addition to the ordinary recruitment faculties of the Presidency of the Council of Ministers, within the annual spending limit of 1,300,000 euros starting from 2018. The related charges are provided pursuant to Article 22.

3. Pending the adoption of the Decree referred to in paragraph 2, the functions of the Italian CSIRT are carried out by the national CERT together with the CERT-PA in collaboration with each other.

4. The Italian CSIRT ensures compliance with the requirements referred to in Annex I, point 1, carries out the tasks referred to in Annex I, point 2, deals with the sectors referred to in Annex II and the services referred to in Annex III and has an appropriate, secure and resilient information and communication infrastructure at the national level.

5. The Italian CSIRT defines the procedures for the prevention and management of IT incidents.

6. The Italian CSIRT guarantees effective, efficient and secure collaboration in the CSIRT network referred to in Article 11.

7. The Presidency of the Council of Ministers communicates to the European Commission the mandate of the Italian CSIRT and the methods of handling incidents entrusted to it.

8. The Italian CSIRT, for the performance of its functions, may also make use of the Agency for Digital Italy.

9. The functions performed by the Ministry of Economic Development as a national CERT pursuant to Article 16a of the Legislative Decree of 1 August 2003, no. 259, as well as those carried out by the Agency for Digital Italy under CERT-PA, pursuant to Article 51 of the Legislative Decree of 7 March 2005, no. 82, are transferred to the Italian CSIRT with effect from the entry into force of the Decree referred to in paragraph 2.

10. For the operating expenses of the Italian CSIRT, the expenditure of 2,700,000 euros is authorised for the year 2018, of which 2,000,000 is for investment expenses, and 700,000 per year starting from the year 2019.
These expenses are provided for pursuant to Article 22.

Art. 9

Cooperation at the national level

1. The competent NIS authorities, the single point of contact and the Italian CSIRT shall collaborate on the fulfilment of the obligations referred to in this Decree. To this end, a technical liaison committee

shall be established at the Presidency of the Council of Ministers, composed of representatives of the competent state administrations pursuant to Article 7, paragraph 1, and of representatives of the Regions and Autonomous Provinces in a number not to exceed two, 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. The organisation of the Committee is defined by Decree of the President of the Council of Ministers, to be adopted upon the proposal of the Ministers for simplification and public administration and economic development, after consultation with the Unified Conference. There are no attendance fees, compensation or reimbursements for participation in the technical liaison committee.

2. Essential service operators and digital service providers shall send incident notifications to the Italian CSIRT.

3. The Italian CSIRT shall inform the competent NIS authorities and the single point of contact about the incident notifications transmitted under this Decree.

Chapter III

Cooperation

Art. 10

Cooperation group

1. The single point of contact shall participate in the activities of the cooperation group composed of representatives of the Member States, the European Commission and the European Union Agency for Network and Information Security (ENISA) and, in particular, contributes to:
a) sharing good practices on the exchange of information relating to the notification of incidents referred to in Article 12 and Article 14;
b) exchanging best practices with Member States and, in collaboration with ENISA, provide support for capacity building in the area of network and information system security;
c) discussing the capacities and state of preparedness of the Member States and evaluate, on a voluntary basis, national strategies for network and information system security and the effectiveness of CSIRTs and identifying best practices;
d) exchanging information and best practices on awareness raising and training;
e) exchanging information and best practices in research and development on network and information system security;
f) exchanging, where appropriate, experiences in network and information security with the relevant institutions, bodies, offices and agencies of the European Union;
g) discussing the standards and specifications referred to in Article 17 with representatives of the relevant European standards organisations;
h) providing information in relation to risks and incidents;
i) examining, on an annual basis, the summary reports referred to in paragraph 4;
l) discussing the work done with regard to exercises relating to network and information systems security, education and training programs, including the activities carried out by ENISA;
m) with the assistance of ENISA, exchanging best practices related to the identification of operators of essential services by Member States, including in relation to cross-border dependencies on risks and incidents;
n) discussing modalities for the communication of notifications of incidents referred to in Articles 12 and 14.

2. The competent NIS authorities, through the single point of contact, ensure participation in the cooperation group in order to develop and adopt guidelines on the circumstances in which operators

of essential services are required to notify incidents, including the parameters referred to in Article 12, paragraph 8.

3. The single point of contact, where necessary, requests the relevant NIS competent authorities, as well as the CSIRT, to participate in the cooperation group.

4. By 9 August 2018 and annually thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of the reported incidents and the actions taken pursuant to Articles 12 and 14.

Art. 11

CSIRT network

1. The Italian CSIRT participates in the CSIRT network, composed of representatives of the CSIRTs of the Member States and of the CERT-EU.

2. The Italian CSIRT, for the purposes of paragraph 1, provides for:
a) the exchange of information on CSIRT services, operations and cooperation capacities;
b) upon the request of the representative of a CSIRT of a Member State potentially affected by an incident, the exchange and discussion of commercially non-sensitive information related to that incident and the associated risks, except in cases where the exchange of information could jeopardise the investigation of the incident;
c) the exchange and making available on a voluntary basis of non-confidential information on individual incidents;
d) upon the request of a representative of a CSIRT from another Member State, the discussion and, where possible, the identification of coordinated intervention for an incident detected in the jurisdiction of that same Member State;
e) the provision of support to other Member States in dealing with cross-border incidents on the basis of voluntary mutual assistance;
f) the discussion, examination and identification of further forms of operational cooperation, also in relation to:
1) categories of risks and incidents;
2) early warning;
3) mutual assistance;
4) principles and methods of coordination, when Member States intervene in relation to cross-border risks and incidents;

g) the informing the cooperation group about its activities and further forms of operational cooperation discussed on the basis of letter f) and the request for guidance on the matter;
h) the discussion of the lessons learned from the exercises on network and information system security, including those organised by ENISA;
i) the formulation of guidelines aimed at facilitating the convergence of operational practices in relation to the application of the provisions of this article on operational cooperation.

Chapter IV

Security of the network and information systems of operators of essential services

Art. 12

Obligations regarding security and notification of incidents

1. The operators of essential services shall adopt adequate and proportionate technical and organisational measures to manage the risks posed to the security of the network and the information systems they use in their operations. Taking into account the most up-to-date knowledge on the

subject, these measures ensure a level of security of the network and information systems adequate to the existing risk.

2. Operators of essential services adopt adequate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of essential services, in order to ensure the continuity of these services.

3. In adopting the measures referred to in paragraphs 1 and 2, operators of essential services shall take into account the guidelines prepared by the cooperation group referred to in Article 10, as well as the guidelines referred to in paragraph 7.

4. Without prejudice to the provisions of paragraphs 1, 2 and 3, the competent NIS authorities may, if necessary, define specific measures, having consulted the operators of essential services.

5. Operators of essential services shall notify the Italian CSIRT and, for information, the competent NIS authority, without undue delay, any incidents that have a significant impact on the continuity of the essential services provided.

6. The Italian CSIRT shall promptly forward notifications to the body set up at the Information Security Department in charge, pursuant to the directives of the President of the Council of Ministers, adopted after hearing the Interministerial Committee for the Security of the Republic (CISR), of the activities of prevention and preparation for any crisis situations and of activation of alert procedures.

7. The notifications include information that allows the Italian CSIRT to determine a possible cross-border impact of the incident. The notification does not expose the party to a liability greater than that resulting from the incident.
The Competent NIS Authorities may establish guidelines for incident reporting.

8. In order to determine the significance of the impact of an incident, the following parameters, in particular, shall be taken into account:
a) the number of users affected by the disruption of the essential service;
b) the duration of the incident;
c) the geographical spread in relation to the area affected by the incident.

9. Based on the information provided in the notification by the operator of essential services, the Italian CSIRT shall inform any other interested Member States where the incident has a material impact on the continuity of essential services.

10. For the purposes of paragraph 9, the Italian CSIRT shall preserve, in accordance with European Union law and national legislation, the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in the notification in accordance with Article 1, paragraph 5.

11. Where circumstances allow, the Italian CSIRT shall provide the operator of essential services, which makes the notification, with relevant information relating to the follow-up to the notification itself, as well as information that may facilitate the effective handling of the incident.

12. Upon the request of the competent NIS authority or the Italian CSIRT, the single point of contact shall transmit, after verification of the conditions, the notifications to the single points of contact of the other Member States concerned.

13. Subject to evaluation by the body referred to in paragraph 6, the competent NIS authority, in agreement with the Italian CSIRT, after consulting the notifying essential service operator, may inform the public about individual incidents, when awareness is needed to avoid an incident or manage an ongoing accident.

14. The implementation of this article must not result in new or greater burdens on public finance. Operators of essential services shall fulfil the obligations provided for in this article on the basis of the financial resources available on their financial statements.

Art. 13

Implementation and control

1. The competent NIS authorities assess compliance by operators of essential services with the obligations set out in Article 12, as well as the related effects on the security of the network and information systems.

2. For the purposes of paragraph 1, operators of essential services are required to provide the competent NIS authority with:
a) the information necessary to assess the security of their network and information systems, including documents relating to security policies;
b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent NIS authority or by a licensed auditor and, in the latter case, make the results, including supporting evidence, available to the competent NIS authority.

3. When requesting the information or evidence referred to in paragraph 2, the competent NIS authority shall indicate the purpose of the requests by specifying the type of information to be provided.

4. Following the evaluation of the information or the results of the security audits referred to in paragraph 2, the competent NIS authority may issue binding instructions for operators of essential services in order to remedy the shortcomings identified.

5. In cases of incidents involving violations of personal data, the competent NIS authority shall work in close cooperation with the Guarantor for the protection of personal data.

Chapter V

Security of the network and information systems of digital service providers

Art. 14

Obligations regarding security and notification of incidents

1. Digital service providers shall identify and adopt adequate and proportionate technical and organisational measures to manage the risks relating to the security of the network and information systems that they use in the context of the offer of services referred to in Annex III within the European Union.

2. Taking into account the most up-to-date knowledge on the subject, these measures ensure a level of security of the network and information systems adequate to the existing risk and take into account the following elements:
a) the safety of systems and facilities;
b) handling of incidents;
c) management of business continuity;
d) monitoring, auditing and testing;
e) compliance with international standards.

3. Digital service providers shall take measures to prevent and minimise the impact of incidents affecting the security of the network and information systems of the digital service provider on the services listed in Annex III offered within the European Union, in order to ensure the continuity of these services.

4. Digital service providers shall notify the Italian CSIRT and, for information, the competent NIS authority, without undue delay, of the incidents having a significant impact on the provision of a service referred to in Annex III that they offer within the European Union.

5. The notifications include information that allows the Italian CSIRT to determine the relevance of a possible cross-border impact. The notification does not expose the party to a liability greater than that resulting from the incident.

6. The Italian CSIRT shall promptly forward notifications to the body referred to in Article 12, paragraph 6.

7. In order to determine the significance of the impact of an incident, the following parameters, in particular, shall be taken into account:
a) the number of users affected by the incident, in particular users that rely upon the digital service for the provision of their services;
b) the duration of the incident;
c) the geographical spread in relation to the area affected by the incident;
d) the extent of the disruption to the operation of the service;
e) the extent of the impact on economic and social activities.

8. The obligation to provide notification about an incident applies only if the digital service provider has access to the information necessary to assess the impact of an incident with reference to the parameters referred to in paragraph 7.

9. If an operator of essential services relies upon a third-party supplier of digital services for the provision of a service that is essential for the maintenance of fundamental economic and social activities, the operator itself shall provide notification of any impact relevant to the continuity of essential services due to an accident involving that operator.

10. If the incident referred to in paragraph 4 concerns two or more Member States, the Italian CSIRT shall inform the other Member States involved.

11. For the purposes of paragraph 9, the Italian CSIRT shall protect, in compliance with European Union law and national legislation, the security and commercial interests of the digital service provider as well as the confidentiality of the information provided.

12. Subject to evaluation by the body referred to in Article 12, paragraph 6, the competent NIS authority, in agreement with the Italian CSIRT, after having consulted the digital service provider concerned and, where appropriate, the competent authorities or the CSIRTs of the other Member States concerned, may inform the public about individual incidents or ask the digital service provider to do so, if awareness is needed to avoid an incident or manage an ongoing one, or if there is in any case a public interest in disclosing the incident.

13. Digital service providers shall apply the provisions implementing the implementing acts of the European Commission, which further specify the technical-organisational measures referred to in paragraph 1 and the parameters, including formats and procedures, relating to the notification obligations referred to in paragraph 4.

14. Without prejudice to the provisions of Article 1, paragraph 7, no additional security or notification obligations are imposed upon digital service providers.

15. This chapter does not apply to micro and small enterprises as defined in the European Commission recommendation of 6 May 2003, no. 2003/361/EC.

Art. 15

Implementation and control

1. In the event that the failure of the digital service providers to comply with the obligations referred to in Article 14 is proven, the competent NIS authority may adopt ex-post supervisory measures appropriate to the nature of the services and operations. Proof of non-compliance with obligations may be produced by the competent authority of another Member State in which the service is provided.

2. For the purposes of paragraph 1, digital service providers are required to:
a) provide the information necessary to assess the security of their network and information systems, including documents relating to security policies;
b) remedy any failure to fulfil the obligations referred to in Article 14.

3. If a digital service provider has its main establishment or a representative in a Member State, but its network or information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of the aforementioned other Member States shall cooperate and assist each other as needed. Such assistance and cooperation may include exchanges of information between the competent authorities concerned and requests to adopt the supervisory measures referred to in paragraph 1.

Art. 16

Jurisdiction and territory

1. For the purposes of this decree, a digital service provider shall be considered subject to the jurisdiction of the Member State in which it has its main establishment. However, a digital service provider is considered to have its main establishment in a Member State when it has its registered office in that Member State.

2. A digital service provider that is not established in the European Union, but offers services listed in Annex III within the European Union, shall designate a representative in the European Union.

3. The representative is established in one of those Member States where the services are offered. The digital service provider shall be considered to be subject to the jurisdiction of the Member State in which its representative is established.

4. The designation of a representative by a digital service provider is without prejudice to legal actions that may be brought against the digital service provider itself.

Chapter VI

Standardisation and voluntary notification

Art. 17

Standardisation

1. For the purposes of harmonised implementation of Article 12, paragraphs 1 and 2, and Article 14, paragraphs 1, 2 and 3, the competent NIS authorities shall promote the adoption of European or internationally accepted standards and specifications relating to security of the network and information systems, without imposing or creating discrimination in favour of the use of a particular type of technology.

2. The competent NIS authorities shall take into account the opinions and guidelines prepared by ENISA, in collaboration with the Member States, regarding the technical sectors to be taken into consideration in relation to paragraph 1, as well as existing standards, including national standards, which could be applied to these sectors.

Art. 18

Voluntary notification

1. Entities that have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services that they provide.

2. In the processing of notifications, the Italian CSIRT shall apply the procedure referred to in Article 12.

3. Mandatory notifications shall be treated as a priority over voluntary notifications.

4. Voluntary notifications shall be processed only if such processing does not constitute a disproportionate or excessive burden.

5. Voluntary notification cannot have the effect of imposing upon the notifying entity any obligation to which it would not have been subjected had it not made such notification.

Chapter VII

Final provisions

Art. 19

Powers of inspection

1. The inspection and verification activities necessary for the measures provided for in Articles 12, 13, 14 and 15, without prejudice to the powers and responsibilities of the bodies responsible for the protection of public order and security, are carried out by the competent NIS authorities.

2. With the subsequent Agreement between the Government, the Regions and the Autonomous Provinces of Trento and Bolzano, uniform criteria shall be defined at national level for carrying out the inspection and verification activities, necessary for the measures provided for in Articles 12, 13, 14 and 15, which concern the networks and information systems used by operators providing health care activities, as well as in relation to the drinking water supply and distribution sector.

Art. 20

Competent authority and regime for ascertaining and imposing administrative sanctions

1. The competent NIS authorities referred to in Article 7, paragraph 1, letters a), b), c), d) and e), for the respective sectors and subsectors of reference set out in Annex II and for the services referred to in Annex III, are competent to ascertain violations and to impose the administrative sanctions provided for in this Decree.

2. For the purposes of ascertaining and imposing the administrative sanctions referred to in paragraph 1, the provisions shall be observed as contained in Chapter I, sections I and II, of the law of 24 November 1981, no. 689.

Art. 21

Administrative sanctions

1. Unless the fact constitutes a crime, the operator of essential services that does not adopt adequate and proportionate technical and organisational measures to manage the risk for the security of the network and information systems, pursuant to Article 12, paragraph 1, is subject to a pecuniary administrative sanction from 12,000 to 120,000 euros. The sanction is reduced by a third if the same act is committed by a digital service provider, in violation of the obligations referred to in Article 14, paragraph 1.

2. Unless the fact constitutes a crime, the operator of essential services that does not adopt adequate measures to prevent and minimise the impact of incidents affecting the security of the network and the information systems used for the provision of essential services, pursuant to Article 12, paragraph 2, is subject to a pecuniary administrative sanction from 12,000 to 120,000 euros. The sanction is reduced by a third if the same act is committed by a digital service provider, in violation of the obligations referred to in Article 14, paragraph 3.

3. Unless the fact constitutes a crime, the essential service operator that does not notify the Italian CSIRT of incidents having a significant impact on the continuity of the essential services provided, pursuant to Article 12, paragraph 5, is subject to a pecuniary administrative sanction from 25,000 to 125,000 euros.

4. Unless the fact constitutes a crime, the essential service operator that does not comply with the obligations, pursuant to Article 13, paragraph 2, is subject to a pecuniary administrative sanction from 12,000 to 120,000 euros.

5. Unless the fact constitutes a crime, the essential service operator that does not comply with the instructions, pursuant to Article 13, paragraph 4, is subject to a pecuniary administrative sanction from 15,000 to 150,000 euros.

6. Unless the fact constitutes a crime, the digital service provider that does not notify the Italian CSIRT of incidents having a significant impact on the provision of a service provided, pursuant to Article 14, paragraph 4, is subject to a pecuniary administrative sanction from 25,000 to 125,000 euros.

7. Unless the fact constitutes a crime, the operator of essential services dependent upon third parties that provides digital services for the provision of a service that is indispensable for the maintenance of fundamental economic and social activities, that fails to notify, pursuant to Article 14, paragraph 9, is subject to a pecuniary administrative sanction ranging from 12,000 to 120,000 euros.

8. Unless the fact constitutes a crime, the digital service provider that does not comply with the obligations, pursuant to Article 15, paragraph 2, is subject to a pecuniary administrative sanction from 12,000 to 120,000 euros.

9. There is a reiteration of the violations referred to in this Article in the cases regulated by Article 8a of the law of 24 November 1981, no. 689. A recurrence leads to an increase of up to three times the envisaged sanction.

Art. 22

Financial provisions

1. The charges deriving from Articles 7 and 8, equal to 5,300,000 euros for the year 2018 and 3,300,000 euros per year starting from 2019, are provided by means of a corresponding reduction in the Fund for the transposition of the European legislation referred to in Article 41a of the law of 24 December 2012, no. 234.

2. The ICT expenses incurred by public administrations pursuant to Articles 7, 8 and 12 of this Decree and more generally the ICT expenses incurred for the adaptation of information systems to this Decree are consistent with the three-year plan for information technology in the public administration pursuant to paragraphs 512 to 520, of Article 1, of the Law of 28 December 2015, no. 208.

3. From the implementation of this decree, with the exclusion of Articles 7 and 8, there must be no new or greater burdens on public finance and the public administrations must be provided with the human, instrumental and financial resources provided for by current legislation.

4. The Minister of Economy and Finance is authorised to make the necessary budget changes in the estimates concerned.

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

Given in Rome, this day, 18 May 2018

Annex I
(referred to in Art. 8)

REQUIREMENTS AND DUTIES OF THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

The requirements and duties of the CSIRT shall be adequately and clearly defined pursuant to this Decree and the Decree of the President of the Council of Ministers referred to in Art. 8, paragraph 2.

They include the following:

1. Requirements for the CSIRT
a) The CSIRT ensures a high level of availability of its communication services, avoiding single points of failure, and has various means that allow it to be contacted and to contact others at any time. Furthermore, the communication channels shall be clearly specified and well known to their user base and the partners with which they collaborate.
b) The CSIRT premises and supporting information systems are located in secure sites.
c) Business continuity:
i. the CSIRT shall be equipped with an adequate system for managing and forwarding requests in order to facilitate the transition;
ii. the CSIRT shall have sufficient staff to ensure its operations 24 hours a day;
iii. the CSIRT shall operate on the basis of an infrastructure whose continuity is guaranteed. To this end, redundant systems and backup workspaces must be available.
d) the CSIRT has the option, if it so desires, of participating in international cooperation networks.

2. Tasks of the CSIRT
a) The tasks of the CSIRT include at the minimum:
i. national incident monitoring;
ii. issuing early warnings, alerts, announcements and disclosures of information to interested parties about risks and incidents;
iii. intervention in the event of an incident;
iv. dynamic analysis of risks and incidents, as well as situational awareness;
v. participation in the CSIRT network;
b) the CSIRT shall establish cooperative relationships with the private sector;
c) To facilitate cooperation, the CSIRT promotes the adoption and use of common or standardised practices in the following areas:
i. procedures for handling incidents and risks;
ii. incident, risk and information classification systems.

Annex II
(referred to in Article 3, paragraph 1, letter g)

OPERATORS OF ESSENTIAL SERVICE

Sector	Subsector	Type of entity
1. Power	a) Electric power	Electricity company as defined in Article 2, paragraph 25 l, of the Legislative Decree of 16 March 1999, 79, which

		carries out “supply”, activities as in Article 2, paragraph 25e, of this Legislative Decree Distribution system managers as defined in Article 2, paragraph 25b, of Legislative Decree of 16 March 1999, 79 Transmission system operators as defined in Article 2, paragraph 25a, of the Legislative Decree of 16 March 1999, 79
	b) Oil	Operators of pipelines Operators of oil production, refining, treatment, storage and transportation facilities
	c) Gas	Supplier companies as defined in Article 2, paragraph 1, letter kk f), of the Legislative Decree of 23 May 2000, no. 164 Distribution system managers as defined in Article 2, paragraph 1, letter kk e), of Legislative Decree of 23 July 2000, no. 164 Transmission system operators as defined in Article 2, paragraph 1, letter kk c), of Legislative Decree of 23 July 2000, no. 164 Storage facility operators as defined in Article 2, paragraph 1, letter kk h), of Legislative Decree of 23 July 2000, no. 164 LNG system operators as defined in Article 2, paragraph 1, letter kk i), of the Legislative Decree of 23 May 2000, no. 164 Natural gas companies as defined in Article 2, paragraph 1, letter t), of the Legislative Decree of 23 May 2000, no. 164 Refining and treatment plant operators of natural gas
2. Transport	a) Air transport	Air carriers as defined in Article 3, first paragraph, number 4) of Regulation (EC) no. 300/2008 of the European Parliament and Council Airport operators as defined in Article 72, paragraph 1, letter b), of the Decree-Law of 24 January 2012, no. 1, converted with modifications, by the Law of 24 March 2012, no. 27, airports as defined in Article 72, paragraph 1, letter a), of this Decree Law, including the central airports referred to in Annex II, point 2 of Regulation (EU) no. 1315/2013 of the European Parliament and Council, and entities that manage related plants located in airports Operators engaged in traffic management control providing air traffic control services as defined in Article 2, first paragraph, number 1), of Regulation (EC) no. 549/2004 of the European Parliament and Council

	b) Rail transport	Infrastructure managers as defined in Article 3, paragraph 1, letter b), of the Legislative Decree of 15 July 2015, no. 112 Railway companies as defined in Article 3, paragraph 1, letter a), of the Legislative Decree of 15 July 2015, no. 112, including operators of service facilities as defined in Article 3, paragraph 1, letter n), of the Legislative Decree of 15 July 2015, no. 112
	c) Transport by waterways	Shipping companies for the transport by inland, maritime and coastal transport of passengers and goods as defined in Annex I of Regulation (EC) no. 725/2004 of the European Parliament and Council, excluding individual ships managed by that Company Port management bodies as defined in Article 2, paragraph 1, letter a), of the Legislative Decree of 6 November 2007, no. 203, including related port facilities as defined in Article 2, first paragraph, number 11), of Regulation (EC) no. 725/2004), and entities that manage works and equipment inside ports Maritime traffic assistance service managers as defined in Article 2, paragraph 1, letter p), of Legislative Decree of 19 August 2005, no. 196
	d) Road transport	Road authorities as defined in Article 2, point 12 of the Delegated Regulation (EU) 2015/962 of the Commission responsible for monitoring traffic management Intelligent transport system operators as defined in Article 1, paragraph 1, letter a), of the Decree of the Minister of Infrastructure and Transport of 1 February 2013
3. Banking sector		Credit institutions as defined in Article 4, paragraph 1, number 1), of Regulation (EU) no. 575/2013 of the European Parliament and the Council
4. Financial market infrastructure		Managers of trading venues as defined in Article 1, paragraph 5 g, letter c), of the Legislative Decree of 24 February 1998, no. 58 Central counterparty as defined in Article 2, first paragraph, number 1), of Regulation (EC) no. 648/2012 of the European Parliament and Council
5. Healthcare sector	Health institutions (including hospitals and private clinics)	Health care providers as defined in Article 3, paragraph 1, letter h), of the LegislativeDecree of 4 March 2014, no. 38
6. Supply and distribution of drinking water		Suppliers and distributors of water intended for human consumption, as defined in Article 2, paragraph 1, letter a), of the Legislative Decree of 2 February 2001, no. 31, but excluding distributors for whom the distribution of water intended for human consumption is only a part of their general activity of distribution of other products and goods that are not considered essential services

7. Digital infrastructure		IXP DNS TLD

Annex III

(referred to in Art. 3, paragraph 1, letter h)

TYPES OF DIGITAL SERVICES

1. Online market
2. Online search engine
3. Cloud computing services