CHIOMENTI

Newsletter

IP, TMT and Data Protection Department
July 2021

Summary

Introduction

The growing number of rules on the cybersecurity outlines with increasing accuracy the framework of the new discipline that will be applied in the next years, also by defining roles and attributions of the main actors, public and private, involved in the safeguard of the security of the digital ecosystem.

The institution of the Agency for the National Cybersecurity and the recent innovations regarding the perimeter of national cybersecurity – briefly analyzed below – confirm the attention of the Italian legislator to the protection of the public interests that come into play in the handling of the current risks on the security of IT systems.

An Agency for the National Cybersecurity has been established

As part of the definition of the new cybersecurity framework and the related national architecture, the Decree-Law of June 14, 2021, no. 82 ("**Decree-Law**") established the Agency for the National Cybersecurity (the ("**ANC**" or "**Agency**"). This is also a significant innovation in the context of the digital transformation activities envisaged in the Italian National Recovery and Resilience Plan. To complete the sectorial

discipline that is being layered with a growing proliferation of provisions provided by decrees-laws and decrees of the President of the Council of Ministers (for an analysis of which see also our previous article available at this link), the protection of national interests in this field and the strict surveillance of compliance is in fact attributed to a new specialized body.

In particular, art. 5 of the Decree-Law expressly provides that at the head of the newly established Agency, based in Rome and endowed with legal personality of public law and regulatory and administrative autonomy, there will be a General Director, to be identified among candidates who have a high level of experience in the management of innovative processes. The President of the Council of Ministers is exclusively responsible for the appointment and revocation of the General Director, as well as the Deputy General Director, and their assignments have a duration of four years, renewable once and therefore for a maximum of a further four years. The General Director of the ANC has the legal representation of the Agency and will also constitute, by express provision of the Decree-Law, "the direct referent of the President of the Council of Ministers" and of the Delegated Authority for the Security of the Republic established by Law no. 124/2007.

Pending the issuance of a regulation that will govern in detail the organization and functioning, the ANC is entrusted with a wide spectrum of important functions, including (a) the exercise of the functions of national authority for cybersecurity, with particular regard to the coordination, also through the promotion of joint actions, between the national public subjects tasked with monitoring duties (first of all the Ministry of the Internal Affairs), (b) the elaboration of a national strategy for the development of cybersecurity that will be adopted by the President of the Council of Ministers, (c) the support to the functions of prevention and preparation for possible crisis situations delegated to the Nucleus for cyber-security set up within the ACN itself, as set out by art. 8 of the Decree-Law, (d) the exercise of the supervisory and sanctioning functions provided by the legislative decree transposing the NIS Directive in Italy (Legislative Decree of May 18, 2018, no. 65) and the decree that recently established the national cyber security perimeter (Decree-Law of September 21, 2019, no. 105, converted by Law of November 18, 2019, no. 133).

In addition, the Agency inherits from the Ministry of Economic Development all the functions previously attributed to that Ministry in the cybersecurity field, and in particular those relating to the national cybersecurity perimeter, the protection of the security and integrity of electronic communications networks pursuant to the relevant legal and regulatory framework (Legislative Decree of August 1, 2003, no. 259), as well as the functions relating to the security of networks and information systems established by the aforementioned Legislative Decree no. 65/2018. The ANC incorporates also all the functions on the matter previously attributed to the Presidency of the Council of Ministers on the perimeter of national cyber security, as well as those initially assigned to the Department of Information for Security ("**DIS**") and the Agency for a Digital Italy ("**AgID**").

Finally, the ANC is entrusted with further institutional tasks of promotion and coordination of an updated and coherent national framework that is able to promptly adapt to the evolutions and developments of the sector, functions of international cooperation in the field of cybersecurity and the development of an awareness in the area of cybersecurity, also through the education of new professional figures.

In order to fully understand the shape and the attributions of the ANC it will be necessary to wait for the conversion of the Decree-Law, which must take place by August 13, 2021, but the decision of the Government to establish a specific sectoral body in charge of the protection of cybersecurity and empowered with the necessary powers represents a clear demonstration of the priority importance that is being given to the protection of the digital space and its continuous evolution.

DECREE ON INCIDENT NOTIFICATIONS AND SECURITY MEASURES RELEVANT TO THE ITALIAN CYBERSECURITY PERIMETER

On 14 June 2021, Decree No. 81 of the President of the Council of Ministers of 14 April 2021 (hereinafter, the "**DPCM**") was published in the Official Gazette, containing the "*Regulation on notifications of incidents impacting on networks, information systems and IT services referred to in Article 1, paragraph 2, letter b), of Law Decree No. 105 of 21 September 2019, converted, with amendments, by Law No. 133 of 18 November 2019, and measures to ensure high levels of security*" (the "**Regulation**").

The DPCM implements the discipline of the Italian national cybersecurity perimeter set out in Law Decree No. 105 of 21 September 2019 (hereinafter, the "**Perimeter**"), in two respects: **(i)** on the one hand, by defining the obligations to notify incidents impacting on the networks, information systems and IT services dedicated to the exercise of an essential function of the State, or to the provision of an essential service, and **(ii)** on the other hand, by indicating a number of security measures that public and private operators included in the Perimeter are required to adopt.

Incident reporting obligations.

In relation to the first item, the Regulation provides that the notification obligations will become fully binding only as of 1 January 2022. For the period between the date of transmission of the list of ICT assets (which is an obligation to which all entities included in the Perimeter are bound) and 31 December 2021, a transitional period is instead identified, in which such entities will still be required to proceed with the notification of security incidents, but "*on an experimental basis*". Indeed, notifications in the transitional period will not be relevant for compliance with the notification obligations under Legislative Decree 65/2018 (in the context of NIS regulation) and under Legislative Decree no. 259/2003 (Electronic Communications Code), which shall be thus complied with separately.

Notifications of security incidents – to be made through specific communication channels and in accordance with the methods defined by the Italian CSIRT (*i.e.* the *Computer Security Incident Response Team* established pursuant to Legislative Decree 65/2018) – are subject to different timeframes in relation to the classification of the categories of incidents, and related severity, contained in Annex A to the Regulation.

Most notably, the Regulation provides that notifications must take place:

(i) within six hours, for the incidents identified in Table 1 of Annex A to the Regulation (which includes, for example, initial exploitation events, failures, privilege exclusion, persistence and evasion of defences, credential collection and lateral movements, exfiltrations);

(ii) within one hour, for the incidents identified in Table 2 of Annex A to the Regulation (which includes events of inhibition of response functions, impairment of control processes, intentional disruption, violation of expected service levels, disclosure of corrupted data or performance of corrupt operations, unauthorised disclosure of digital data.

The Regulation clarifies that the aforesaid time limits run from the moment when the entities included in the Perimeter became aware of them, following the evidence obtained (also through the monitoring tests and controls carried out on the basis of the security measures referred to *below*).

The notification shall be supplemented *(a)* promptly, if the entity becomes aware of new significant elements (*e.g.*, specific vulnerabilities exploited or indicators of compromise (IOC) detected, etc.); *(b)* within six hours, upon request by the Italian CSIRT.

The entity that has suffered an incident shall also promptly notify the Italian CSIRT of the implementation plans of the activities to restore the ICT assets affected by the incident, as soon as they have been defined and started. If so requested by the Italian CSIRT, the entity shall also submit, within 30 days from the request, a technical report illustrating the significant elements of the incident and the remediation actions taken.

In addition to the cases of compulsory notification, the Regulation provides also for the possibility of notifying – on a voluntary basis – incidents which are not indicated in the tables in Annex A, or incidents which, although falling within the categories of Annex A, affect networks, information systems and information services other than ICT assets relevant to the Perimeter. In this regard, the DPCM expressly sets forth that such voluntary notifications cannot impose on the notifying entity obligations, to which the entity would not have been subject had it not made such notification.

Lastly, the Regulation is without prejudice to the application of the provisions set out in Law No. 124/2007 and the relevant implementing provisions, concerning incidents relating to networks, information systems and IT services that are relevant to the management of classified information.

Obligations regarding security measures.

In relation to the second item, the Regulation requires the entities included in the Perimeter to adopt specific security measures for each ICT asset in scope. The security measures covered by these obligations (divided into functions, categories, subcategories, points and letters) are detailed in Annex B to the Regulation.

Depending on the categories of security measures concerned, the Regulation sets forth different timeframes that the entities included in the Perimeter are required to respect in order to adopt them. Most notably, the following deadlines must be complied with, to be calculated from the date of transmission of the lists of ICT assets provided for by the rules on the Perimeter, or from the date of entry into force of the Regulation (if the transmission of the lists of ICT assets took place on an earlier date):

(i) within six months, as regards the less burdensome security measures belonging to category A as set out in Appendix 2 of Annex B) – including, for example, measures for the mapping of systems, physical equipment and data flows; measures and actions for risk assessment and identification of tolerated risk; measures for user training and education; measures relating to the physical transfer, removal and destruction of storage devices; the presence of incident response and recovery plans, as well as vulnerability management plans; the definition of roles and responsibilities for monitoring processes; etc.;

(ii) within 30 months, as regards the more burdensome security measures (belonging to category B as set out in appendix no. 2 of Annex B) – including, for example, measures for the mapping of the software platforms and applications in use; measures for the identification and prioritization of risk responses; measures relating to the procurement of ICT assets; measures for credential management and access control; data control and protection measures, including the storage of data processed through the use of ICT assets within the national territory or, in certain cases, within the EU territory; existence of procedures and processes for the protection of information; measures concerning the maintenance of information systems and industrial controls; continuous monitoring measures for security; mitigation actions in the event of security events; etc.

When the lists of ICT assets are updated, the entities will also be required to adapt the security measures already adopted, within the same time limits indicated above (which in this case will, however, run from the date on which the lists are updated).

In addition to these obligations, within 60 days from the date of entry into force of the Regulation, the entities included in the Perimeter shall apply a number of minimum security measures (*e.g.*, physical and documentary security measures), as identified in Annex C to the Regulation, to be applied to the information relating to the list of entities included in the Perimeter, the lists of ICT assets, the elements of the notifications made in the event of an incident and to the documentation prepared in implementation of the security measures referred to in Annex B .

Finally, also with respect to the security measures obligations, the Regulation does not affect the application of the provisions of Law no. 124/2007 and the relevant implementing provisions, concerning incidents relating to networks, information systems and IT services that are relevant to the management of classified information.

The text of the DPCM is accessible at this link.

ITALIAN PRIME MINISTER SIGNS THE UPDATE OF THE ITALIAN CYBERSECURITY PERIMETER

On June 15, 2021, the Italian Prime Minister, Mario Draghi, signed the update of the list of subjects included in the perimeter of national cyber security ("**Perimeter**"). The provision, made at the request of the Interministerial Committee for the Security of the Republic ("**CISR**"), entailed an enlargement of the number of public and private entities that, in total, exercise, through networks, information systems and computer services, No. 223 essential functions of the State, or provide services essential for the maintenance of strategic civil, social or economic activities.

It should be reminded that the Perimeter was established pursuant to Article 1, paragraph 1, of Decree-Law No. 105 of 21 September 2019, converted with amendments by Law No. 133 of 18 November 2019. The purpose of the Perimeter is to (i) ensure a high level of security of the networks, information systems and IT services of public administrations, entities and public and private operators with a location in the national territory, on which the exercise of an essential function of the State depends; (ii) ensure the provision of a service essential for the maintenance of civil, social or economic activities that are fundamental to the interests of the State and from whose malfunctioning, interruption, even partial, or improper use, may result in prejudice to national security.

Following the update, the Department of Information Security (*Dipartimento delle Informazioni per la Sicurezza*) will notify the interested parties who, within a period of 6 months, will be required to communicate the networks, information systems and computer services they respectively employ for the provision of essential State functions and services included in the Perimeter.

In addition, as of 23 June 2021, the Perimeter will begin to be "operational" with respect to the subjects entered on 22 December 2020. These subjects will therefore have to apply the required security measures and notify the Italian Computer Security Incident Response Team of any incidents that may occur.

In order to allow adequate organization of the entities included in the Perimeter to comply with the incident reporting procedures, these will proceed on a trial basis until 31 December 2021.

Contacts

Gilberto Nava
Partner – Chiomenti
IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Giulio Vecchi
Counsel – Chiomenti
IP, TMT, Data Protection
T. +39.02.72157.658
giulio.vecchi@chiomenti.net