Source of law	Type of subject	Requirement	Content	Recipient of information	Function	Controls
NIS Directive, art. 14 (1)	Operators of Essential services (OES)	Take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed	Sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity			Having regard to the state of the art, proportionate technical and organisational measures to ensure a level of security of network and information systems appropriate to the risk posed have been adopted.
NIS Directive, art. 14 (2)	OES	Take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services				In order to ensure the continuity of the network and information systems used to provide essential services, appropriate measures to prevent and minimise the impact of incidents have been adopted.
NIS Directive, art. 14 (3)	OES	Notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.				Every incident having a significant impact on the continuity of the essential services provided it is notified, without undue delay, to the competent authority or the CSIRT. Notification includes information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident.
NIS Directive, art. 16 (1)	Digital service providers (DSP)	Identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services	Shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards.			Appropriate and proportionate technical and organisational measures have been adopted to manage the risks posed to the security of network and information systems in use, taking into account: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards.
NIS Directive, art. 16 (2)	DSP	Take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services … with a view to ensuring the continuity of those services.				Measures to prevent and minimise the impact of incidents affecting the security of the network and information systems in order to ensuring the continuity of the essential services provided.
NIS Directive, art. 16 (3)	DSP	Notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service				Any incident having a substantial impact on the provision of an essential service is notified to the the competent authority or the CSIRT without undue delay.
NIS Directive, Art. 15(2) (a)	CSIRT	Have the powers and means to require operators of essential services to provide the information necessary to assess the security of their network and information systems, including documented security policies				Appropriate roles and procedures are defined to obtain from the operators of essential services the information necessary to assess the security of their network and information systems, including documented security policies.
NIS Directive, Art. 15(2) (b)	CSIRT	Powers and means to require operators of essential services to provide evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority				Operators of essential services provide evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor, in order to make the results available to the competent authority.
NIS 2 Directive, Art. 20 (2)	Essential entities (EE) and Important Entities (IE)	Training activities for management bodies of EE and IE (mandatory)				Mandatory training activities for management bodies of EE and IE are carried out.
NIS 2 Directive, Art. 20 (2) -	EE and IE	Training activities for employees (not mandatory)				Training activities for EE and IE employees are carried out.
NIS 2 Directive, Art. 21(a)	EE and IE	policies on risk analysis and information system security;				Risk analysis and information system security policies are adopted by essential and important actors taking into account the most up-to-date knowledge on the subject and, where appropriate, relevant European and international standards, as well as the costs of implementation, to ensure a level of computer and network security appropriate to the existing risks.
NIS 2 Directive, Art. 21(b)	EE and IE	incident handling;				Appropriate and proportionate technical and organisational measures are adopted for incident management, taking into account the most up-to-date knowledge on the subject and, where appropriate, relevant European and international standards, as well as the costs of implementation, to ensure a level of computer and network security appropriate to the existing risks.
NIS 2 Directive, Art. 21(c)	EE and IE	business continuity, such as backup management and disaster recovery, and crisis management;				Appropriate and proportionate technical and organisational measures are adopted to ensure business continuity, such as backup management and disaster recovery, and crisis management, taking into account the most up-to-date knowledge on the subject and, where appropriate, relevant European and international standards, as well as the costs of implementation, to ensure a level of computer and network security appropriate to the existing risks.
NIS 2 Directive, Art. 21(d)	EE and IE	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;				Aappropriate and proportionate technical and organisational measures are adopted to ensure supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
NIS 2 Directive, Art. 21(e)	EE and IE	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;				Appropriate and proportionate technical and organisational measures are adopted to ensure security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.
NIS 2 Directive, Art. 21(f)	EE and IE	policies and procedures to assess the effectiveness of cybersecurity risk-management measures;				Policies and procedures to assess the effectiveness of cybersecurity risk-management measures are adopted.
NIS 2 Directive, Art. 21(g)	EE and IE	basic cyber hygiene practices and cybersecurity training;				Basic computer hygiene practices are adopted and cyber security training is conducted.
NIS 2 Directive, Art. 21(h)	EE and IE	policies and procedures regarding the use of cryptography and, where appropriate, encryption;				Policies and procedures regarding the use of cryptography and, where appropriate, encryption are adopted.
NIS 2 Directive Art. 21(i)	EE and IE	human resources security, access control policies and asset management;				Policies and procedures regarding the human resources security, access control policies and asset management are adopted.
NIS 2 Directive Art. 21(j)	EE and IE	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.				Technichal measures such as multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate have been adopted.
NIS 2 Directive Art. 23(1)	EE and IE	notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services				In the event of an incident with significant impact on the provision of a EE and IE services, a notification is made to the CSIRT or (in case applicable) its competent authority, in accordance with paragraph 4.
NIS 2 Directive Art. 23(1)		notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services.				In the event of an incident with significant impact on the provision of a EE and IE services, a notification is made to the recipients of the services that are adversaly affected without undue delay.
NIS 2 Directive Art. 23(2)		communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat.				In the event of an incident with significant impact on the provision of a EE and IE services, a communication is made to the recipients that are potentially affected by a significant cyber threat regarding any measures or remedies that those recipients are able to take in response to that threat without undue delay.
NIS 2 Directive Art 11 (c)	CSIRT	responding to incidents and providing assistance to the EE and IE concerned, where applicable				Incident response activity and assistance are provided to the EE and IE concerned
NIS 2 Directive art 11 (d)	CSIRT	collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity				Forensic data and a dynamic risk and incident analysis, via a proactive scanning of the network and information systems is carried out.
NIS 2 Directive art 11 (e)	CSIRT	providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;				In case of request by an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact is provided.
NIS 2 Directive art 11 (g)	CSIRT	where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);				Where applicable, The CSIRT act as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1).
NIS 2 Directive art 11(h)	CSIRT	contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).				Activities are carried out to contribute to the deployment of secure information-sharing tools pursuant to Article 10(3).
D.Lgs. n. 65/2018 art. 7	Agenzia per la cybersicurezza nazionale	The National Cybersecurity Agency is designated as the competent national NIS authority. As such, it is responsible for the implementation of the decree with regard to the sectors and supervises the application of this decree at national level, also exercising the relevant inspection and sanctioning powers. The National Cybersecurity Agency is designated as the single point of contact for network and information system security. As such, it performs a liaison function to ensure cross-border cooperation of the NIS competent national authority with competent authorities of other Member States, as well as with the CSIRT cooperation group and network.				
D.Lgs. n. 65/2018 art. 8	Italian CSIRT	The Italian CSIRT is established within the Agenzia per la cybersicurezza nazionale, which performs the tasks and functions of the national Computer Emergency Response Team (CERT). The Italian CSIRT shall ensure compliance with the requirements set out in point 1 of Annex I, perform the tasks set out in point 2 of Annex I, address the areas set out in Annex II and the services set out in Annex III, and have an appropriate, secure, and resilient information and communication infrastructure at national level. The Italian CSIRT defines procedures for the prevention and management of cyber incidents. The Italian CSIRT ensures effective cooperation, efficient and secure cooperation in the CSIRT network				
D.Lgs. n. 65/2018 art. 8	Italian CSIRT	Art. 11: The Italian CSIRT participates in the network of CSIRTs, composed of representatives of the Member States' CSIRTs and the EU-CERT. To this end, it: a) exchanges information on the services, operations and co-operation capabilities of the CSIRTs; b) at the request of the representative of a CSIRT of a Member State potentially affected by an incident, exchanges and discusses non-commercially sensitive information related to that (b) at the request of a representative of a CSIRT of a Member State potentially affected by an incident, exchange and discuss commercially non-sensitive information related to that incident and the associated risks, except in cases where the exchange of information could compromise the investigation of the incident; (c) exchange and make available on a voluntary basis non-confidential information on individual incidents; (d) at the request of a representative of a CSIRT of another Member State, discuss and, where possible, identify a coordinated response to an incident detected in the jurisdiction of that same Member State; (e) provide support to other Member States in dealing with cross-border incidents on the basis of mutual assistance voluntary; f) discuss, examine, and identify further forms of operational cooperation; g) informing the Cooperation Group about its activities and further forms of operational cooperation; h) discussing lessons learned from network and information system security exercises, including those organised by ENISA.				
		operational cooperation; g) informing the Cooperation Group about its activities and further forms of operational cooperation; h) discussing lessons learned from network and information system security exercises, including those organised by ENISA.				

D.Lgs. n. 65/2018 art. 9	Comitato tecnico di raccordo	The sector authorities cooperate with the competent national NIS authority for the fulfilment of the obligations under the decree. To this end, a technical liaison committee is established at the Agenzia per la cybersicurezza nazionale. The Committee is chaired by the NIS competent national authority and is composed of the representatives of the State administrations as sector authorities and of no more than two representatives of the autonomous Regions and Provinces, designated by the autonomous Regions and Provinces at the Permanent Conference for relations between the State, the Regions and the autonomous Provinces of Trento and Bolzano.				
D.Lgs. n. 65/2018 art. 10	Single point of contact	The single point of contact shall contribute to: (a) share good practices on incident reporting; (b) exchange best practices with Member States and, in cooperation with ENISA, provide support for capacity building on NIS; (c) discuss Member States' capabilities and state of preparedness and assess national NIS strategies and the effectiveness of CSIRTs and identify best practices; (d) exchange information and best practices on awareness-raising and training, research and development with regard to NIS; (e) provide information in relation to risks and incidents.				
D.Lgs. n. 65/2018 art. 12	OESs	OESs shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems they use in their operations. OESs shall take appropriate measures to prevent and minimise the impact of security incidents on the network and information systems used for the provision of essential services, in order to ensure the continuity of those services. OESs shall notify the Italian CSIRT without undue delay, incidents with a significant impact on significant impact on the continuity of essential services provided.				
D.Lgs. n. 65/2018 art. 13	OESs	The NIS competent authorities assess the compliance of essential service operators with the obligations, as well as their effects on network and information system security. For these purposes, OESs are required to provide the NIS competent authority with: (a) the information needed to assess the security of their network and information systems, including security policy documents; (b) evidence of the effective implementation of security policies.				
D.Lgs. n. 65/2018 art. 14	DSPs	DSPs shall identify and take appropriate and proportionate technical and organisational measures to manage risks related to the security of the network and information systems they use in the context of offering services within the European Union. Considering the most up-to-date knowledge on the subject, these measures shall ensure a level of network and information system security appropriate to the risk involved and shall take into account the following elements: a) system and facility security; b) incident handling; c) business continuity management; d) monitoring, auditing and testing; e) compliance with international standards. DSPs shall take measures to prevent and minimise the impact of incidents affecting the security of the digital service provider's network and information systems on the services offered within the European Union, to ensure the continuity of these services. DSPs shall notify the Italian CSIRT without undue delay, incidents having a significant impact on significant impact on the provision of a service listed in Annex III that they offer within the European Union.				
d.l. 105 of 2019 art 1 (2) (b)	perimeter subject	List of networks, information systems and information services	draw up and update, at least once a year, a list of the networks, information systems and information services referred to in paragraph 1, for which they are responsible, including their architecture and components			Check if the list of networks, networks systems and information services are up to date at least once a year.
d.l. 105 of 2019 art 1 (3) (a)	Perimeter subject	Notification of incidents	notify the Italian CSIRT of any incidents affecting the networks, information systems and computer services referred to in paragraph 2(b).			-
d.l. 105 of 2019 art 1 (6) (a)	Perimeter subject	Communication of procurement process	communication related to any procurement process addressing ICT goods, systems and services to be used on the networks, information systems and for the performance of the IT services referred to in paragraph 2, letter b). Notification to CVCN shall also include the assessment of the risk associated with the object of the supply, also in relation to the scope of use. Within 45 days (extendable by 15 days) the CVCN may carry out preliminary verifications and impose conditions and tests on hardware and software to be performed also in cooperation with the subjects under paragraph 2, letter a) After 45 days, in case of no reply by CVCN, the parties that have made the notification may continue the procedure. In case of conditions and tests of hardware and software, the relevant notices and contracts shall be supplemented with clauses that make the contract conditional, either suspensively or resolutively, on compliance with the conditions and the favourable outcome of the tests ordered by the CVCN. .			-
DPCM 81 art. 3 cc. 1-4 e d.l. 105 of 2019 art. 1 c. 3-bis (added by d.l. 115 of 2022, better known as decreto aiuti bis)	perimeter subject	Mandatory notification of incidents	Incidents impacting ICT assets within the perimeter or information systems or IT services that share security functions, resources there computation or memory, or basic software (OS or virtualization) with ICT assets must be notified to the CSIRT at the ACN. Notification must be made within six hours (incidents in Table 1 of Annex A) or one hour (incidents in Table 2 of Annex A). Incidents impacting networks, information systems, and IT services of one's own non-perimeter, according to the taxonomy issued by the ACN, must also be notified. Notification must be made within seventy-two hours. Exceptions are incidents impacting DOD networks, information systems, and IT services. The provisions of DPCM 81 should be applied, insofar as they are compatible.	CSIRT at ACN		Check the level of knowledge about the different kinds of incidents to know the deadline of each casuistry.
D.l. 105 of 2019 Art. 1 c. 3-bis (added by Decree Law 115 of 2022, better known as decreto aiuti bis)	ACN (in the figure of the general manager)	Incident taxonomy	The taxonomy of reportable incidents regarding relevant non-perimeter networks, information systems, and IT services should be adopted	perimeter subjects		Check that the list of incident names regarding relevants non perimetral networks, information systems and IT services is up to date.
D.P.C.M. 30 July 2020, no. 131, art. 4	Identified administrations	Art. 4: For the purposes of identifying the entities included in the perimeter, the administrations: a) identify the essential functions and essential services of direct relevance or exercised or provided by supervised entities or operators, including private operators, that depend on networks, information systems or computer services, the interruption or impairment of which could be detrimental to national security; b) for these purposes, assess the effects of the interruption of the function or service, its territorial extension, the potential number of users, the economic repercussions. ...; c) identify the essential functions and services for which, in the event of interruption or impairment, the harm to national security is deemed to be the greatest and the possibilities of minimum mitigation possibilities and rank them on an ascending scale; d) identify the entities performing the essential functions.				
D.P.C.M. 30 July 2020, no. 131, art. 5	Identified administrations	The identified administrations shall prepare a list of entities to be included in the perimeter and transmit it to the CISR, within thirty days of the inclusion of each addressee in the list. The communication shall indicate the essential function or the essential service in relation to the performance of which the entity has been included in the list.				
D.P.C.M. 30 July 2020, no. 131, art. 7	Entities included in the perimeter	The entities included in the perimeter prepare and update, at least once a year, the list of ICT assets under their responsibility, indicating their networks, information systems and IT services.				
DPCM 81 art. 3 c. 5	perimeter subject	Integration of mandatory notification of incidents	Supplementing the notification in a timely manner once additional elements become known	CSIRT at ACN		-
DPCM 81 art. 3 c. 7	perimeter subject	Integration of mandatory request notification of incidents	Supplementation of notification at the request of the CSIRT within six hours of the request, subject to investigative secrecy	CSIRT at ACN		-
DPCM 81 art. 3 c. 8	perimeter subject	Notification of the restoration of impacted ICT assets	Notification of the restoration of impacted ICT assets to the CSIRT at ACN, subject to investigative secrecy	CSIRT at ACN		-
DPCM 81 art. 3 c. 8	perimeter subject	Notification of incident to staff for perimeter implementation	Notification of incident to staff for perimeter implementation (security measure ID.AM-6)	Personnel for perimeter implementation		-
DPCM 81 art. 5 c. 1 and D.l. 65 of 2018 art. 7.	ACN	Forwarding of incident notifications	Forwarding of incident notifications to the body of the Ministry of the Interior for the security and regularity of telecommunications services (Article 7-bis of Decree-Law No. 144 of July 27, 2005, converted, with amendments, by Law No. 155 of July 31, 2005)	Body of the Ministry of the Interior for the safety and regularity of telecommunications services		-
DPCM 81 art. 8 c.1 let. a)	perimeter subject	Implementation of security measures (category A)	Implementation of security measures identified in Annex B Category A within six months from the date of transmission of ICT asset lists			Security measures identified in Annex B category A are checked regularly and implemented within 6 months from the transmission of ICT asset lists.
DPCM 81 art. 8 c. 1 let. b)	perimeter subject	Implementation of security measures (category B)	Implementation of security measures identified in Annex B category B within thirty months from the date of transmission of ICT asset lists			Security measures identified in Annex B category A are checked regularly and implemented within 6 months from the transmission of ICT asset lists.
DPCM 81 art. 8 c. 2	perimeter subject	Notification of successful implementation of security measures	Notification of successful implementation of security measures to ACN through its digital platform	ACN		The level of implementation is notified through ACN digital platform is and kept up to date.
DPCM 81 art. 8 c. 4	perimeter subject	Assessment of the need for implementation of new security measures following the update of the ICT asset list	Assessment of the need for implementation of new security measures as a result of updating the list of ICT assets. If yes, proceed according to the procedures in Art. 8 c. 1	ACN		An assessment of the need for implementations of new security measures is carried out and the implementations are updated within 6 months since the transmission of the ICT list, if it is needed.
DPCM 81 art. 8 c. 5	perimeter subject	Notification of adjustment of security measures	Notification of adjustment of security measures within six months	ACN		-

DPCM 81 art. 9	perimeter subject	Implementation of minimum security measures for information protection (Annex C)	Implementation of the security measures identified in Annex C within sixty days from the effective date of DPCM 81 a: (a) to the list of subjects referred to in Article 1, paragraph 2-bis, of the Decree-Law; (b) to the lists referred to in Article 1, paragraph 2(b), of the Decree-Law, including the description of the architecture and components, as well as the risk analysis (c) to the elements of the notifications made pursuant to Article 3, including the report referred to in Article 3, Paragraph 7; (d) to the model referred to in Article 8, Paragraph 1, and the documentation prepared in implementation of the security measures referred to in Annex B.			Security measures identified in Annex C are checked regularly and implemented within 60 days from the effective date of DPCM 8.1
DPCM 81 art. 9 c. 4 and art. 42 1 124 of 200	perimeter subject	Application of security measures for classified information	If a security classification is applied, the security measures in l. 124 of 2007 apply.			-
DPR 54 art. 3 cc. 4	perimeter subject	Analysis of the relative risk associated with the object of supply	Before proceeding with a supply of ICT goods, systems, and services, intended to be used on perimeter assets and belonging to the categories identified by the DPCM June 15, 2021, a special document for the analysis of the associated risk must be drawn up. The document shall contain a description of the following elements: a) the operational environment of the area of use specifying: 1. the components with which the object of supply interacts and the configurations of these components; 2. any existing physical, technical, procedural, personnel-related security measures with an indication of any certifications or verifications performed; b) the security requirements that characterize the use of the object of supply, expressed in terms of its ability to protect the availability, integrity and confidentiality of information and services referred to in paragraph 3(d).	supplier and central purchasing agency, if any		Before purchasing ICT goods, systems and services intended for the protection of the perimeter, a special document for the analysis of the risk must be drawn up. This document shall contain: (a) operational environment of the area of use: the components that the objects of supply will interact with and their configuration and certifications/verifications related to existing physical, technical, procedural personnel related security measures; (b) the security requirements that characterize the use of the object of supply, in terms of the ability to protect confidentiality, integrity and availability of information.
DPR 54 art. 3 cc. 1-3 and DPR 54 art. 10 cc. 1-2	perimeter subject (with the exception of public security authorities and police forces)	Notice of entrustment	Prior to awarding procedures or conclusion of contracts for the supply of ICT goods, systems, and services, intended to be used on perimeter assets and belonging to the categories identified by the DPCM June 15, 2021, notice shall be given to the CVCN or VCs. The communication shall include the identification data of the perimeter subject and: a) the general description of the object of the supply; b) the use, i.e., the intended use of the object of the supply within the ICT assets referred to in Article 7 of the DPCM; c) the category to which the object of the supply belongs; d) the information and services that the object of the supply is to deal with and the related management methods; and e) information on the possible acquisition through the tools referred to in Article 1, paragraph 512, of Law No. 208 of December 28, 2015. The risk analysis document associated with the object of the supply must be attached to the communication. The communication should not be made if it is indispensable to proceed abroad for the supplies of the following ICT goods, systems and services. It is considered essential to proceed with foreign procurement if the supplies are for: (a) implementation and upgrading of computer and telecommunications networks; (b) connectivity services; and (c) management, support and maintenance services for computer, network and telecommunications equipment and systems, delivered in-person at the foreign location.	CVCN or CV		Before purchasing ICT goods, systems and services intended for the protection of the perimeter, a special document for the analysis of the risk must be drawn up. This document shall contain: (a) operational environment of the area of use: the components that the objects of supply will interact with and their configuration and certifications/verifications related to existing physical, technical, procedural personnel related security measures; (b) the security requirements that characterize the use of the object of supply, in terms of the ability to protect confidentiality, integrity and availability of information.
DPR 54 art. 3 cc. 1-3	CVCN	Methodologies for preparing the risk analysis document and identifying test severity levels	Methodologies for preparing the risk analysis document and identifying test severity levels are to be defined within 60 days after the regulations come into force	perimeter subjects		Identify test severity levels within 60 days after a regulamentation comes into force.
DPR 54 art. 4 cc. 8	CVCN	Testing methodologies	Methodologies for conducting tests should be defined and kept strictly confidential	CVCN, CV or LAP		There must be regular controls on the level of confidentiality of testing methodologies.
DPR 54 art. 5 cc. 4	CVCN	Definition of tests corresponding to severity levels	Within sixty days of the entry into force of the regulations, the CVCN shall define the tests corresponding to the levels of severity	perimeter subjects		To each test there must be a corresponding level of severity.
DPR 54 art. 5 c. 1	perimeter subject	Information needed for preliminary verifications	At the request of the CVCN or a VC, the perimeter entity shall provide the necessary information to ensure cooperation in identifying the conditions for the supplier and the type of hardware and software testing to be performed	CVCN or CV		Perimeter entities must cooperate with CVCN and VC and thus identify the conditions of hardware and software.
DPR 54 art. 3 c. 5	suppliers	Activities preparatory to the execution of the tests	If the CVCN or a VC requires certain tests to be performed as part of the preliminary verifications, the following preliminary activities must be performed: (a) provide evidence of the suitability of the safety functions and their configurations to meet the safety requirements of Article 3(4)(b); (b) provide for the setting up of a test environment adequately representative of the operational reality at the laboratory or, if necessary, at the supplier's or perimeter entity's premises (c) provide a general description of the architecture of the evaluation object and its functions; (d) provide a description of the security features implemented in the evaluation object; (e) provide a description of the functional and security tests already performed by the supplier or manufacturer or a third party, including their results	CVCN or CV		Perform said preliminary activities if requested: (a) suitability of the functions must meet the requirements of article 3; (b) set up a test environment that must be representative of the current operational condition at the laboratory or at the perimeter; (c) a general architecture of the object and its functions must be described; (d) describe the security features implemented in the evaluation object; (e) it must be made clear what are the current security tests and the functional tests performed and the results obtained.
DPR 54 art. 3 c. 4	suppliers	Test execution	If the CVCN or a CV prescribes certain tests to be performed as part of pre-testing, they must be performed	CVCN or CV		Follow the guidelines regarding the tests given by the CVCN or the CV
DPR 54 art. 3 c. 4 and art. 5 c. 6	CVCN or CV	Conclusion of preliminary verifications	Within forty-five days of the notice of award by the perimeter entity, preliminary verifications shall be completed and, if necessary, the following shall be defined: - conditions and tests of hardware and software to be included in the clauses of the notice or contract. The conditions condition suspensively or resolutively the contract; - usage requirements to the perimeter entity An additional extension of fifteen days is possible for the following cases of particular complexity: a) consists of ICT assets, systems, and services integrated with each other; b) is based on newly developed technologies for which established test methodologies are not available; c) interacts with components that deliver other essential functions or services	perimeter subjects		After noticing the award of a perimeter entity there are 45 days to ensure preliminary verifications, these shall define: usage requirements of the perimeter entity and the conditions and tests of hardware and software to be included in the clauses of the contract. In cases of particular complexity an extensions of 15 days is possible. Those cases can be: (a) ICT assets, systems, and services integrated with each other; (b) new developed technologies for which establish testing is not yet developed; (c) interactions of the supplies with other essential functions or services.
DPR 54 art. 5 c. 8	subject perimeter	Indication of the security requirements of the supply object	The perimeter entity conducting a bidding procedure or entering into a contract, either directly or through central purchasing bodies, shall indicate the security requirements of the object of supply, taking appropriate confidentiality precautions	supplier and central purchasing agency, if any		Confidentiality precaution is taken when indicating the requirements of the object of supply.
DPR 54 art. 5 c. 7	central purchasing bodies	Compliance with the provisions of DPR 54	Central purchasing bodies shall apply the provisions of DPR 54 with reference to the procurement of ICT goods, systems and services intended for use on perimeter assets and belonging to the categories identified by the Prime Minister's Decree of June 15, 2021			-
DPR 54 art. 5 c. 9	subject perimeter	Disclosure of supplier and supply references	Once the tender award has been made or the contract has been concluded, the perimeter entity shall notify the CVCN or VCs of the supplier's references and any useful element to uniquely identify the supply object	CVCN or CV		The supplier's reference is notified to the CVCN or the CV by the Perimeter entities once the contract has been concluded.
DPR 54 art. 6 c. 6	ACN	Development of the IT platform to support the CVCN and CVs.	ACN develops and maintains platform to support CVCN and VCs to receive foster care notices	CVCN or CV		-
DPR 54 art. 6 c. 1	CVCN or CV	Verification of previous evaluations	When the CVCN or a CV receives references from a supplier and a supply, it verifies whether that supply has already undergone security assessments or if there are controls in place			Each time references are received from a supplier, it must be verified wether that supply has already undergone security processes or if there are controls taking place.
DPR 54 art. 6 c. 4	CVCN or CV	Additional tests	If implementation tests and intrusion tests for severity levels not less than those selected have not been performed on all security functions necessary to meet security requirements, new supplementary tests should be indicated, excluding previous	perimeter subjects		If implementation tests and intrusion tests for severity levels not less than those selected have not been performed on all security functions necessary to meet security requirements, new supplementary tests are indicated.
DPR 54 art. 6 c. 5 and DPR 54 art. 7 c. 1	CVCN or CV	Notification of completion of test preparation phase	If implementation tests and intrusion tests for levels of severity not less than those selected have not been performed on all security functions necessary to meet security requirements, the perimeter entity and the vendor should be notified of the conclusion of the process. If necessary, there may be usage prescriptions. After any additional prescribed tests have been completed, the perimeter entity and the supplier should be notified of the conclusion of the proceeding.	perimeter subjects and suppliers		The conclusion of all requested implementation tests and intrusion tests are notified to the vendor. If any additional prescribed testa have been completed, the perimeter entity and the supplier are notified.
DPR 54 art. 7 c. 1-3 and DPR 54 art. 4 c. 5	CVCN or CV	Notification of start of testing	The start of testing, to be completed within sixty days from the date the perimeter entity makes the evaluation object available, must be communicated to the perimeter entity and supplier. Arrangements for collaboration with suppliers during the execution of the tests must be specified. Where possible, tests are performed at the CVCN, a VC or LAP, otherwise at the perimeter subject or a supplier	perimeter subjects and suppliers		After the perimeter entity makes the evaluation object available, the start of testing must be completed within sixty days, notifying perimeter entities and suppliers. CVCN, VC, LAP should be favoured for testing. In case this is not possible, tests can be performed on perimeter subjects or suppliers.
DPR 54 art. 7 cc. 5,8	CVCN or CV or LAP	Notification of malfunction	In case of malfunction of the evaluation object or the test environment prepared by the supplier, the person included in the perimeter and the supplier shall be promptly notified of the reasons against the continuation of testing. The sixty-day period for execution shall be suspended for a maximum of ten days, during which the supplier may arrange to resolve the malfunction. If a solution cannot be found within this period,	Perimeter subjects and providers and (CVCN if the appointee was the LAP)		Whenever the evaluation object or test environment prepared by the supplier meets a malfunction, the supplier is promptly notified. After that, an extension of a maximum of 10 days, over the sixty days period, might be implemented, during which the suppliers should resolve the malfunction.
DPR 54 art. 7 c. 5	supplier	Troubleshooting	Upon receipt of notice from the CVCN or a CV, the provider shall resolve the malfunction	CVCN or CV		In case the supplier cannot find a solution is 10 days, CVCN and CV is notified and the supplier will be helped by them to find a solution.
DPR 54 art. 7 c. 5	CVCN or CV	Notification of termination of the test execution phase due to malfunction	If the malfunction cannot be resolved within the time limit, notice is given to end the test execution phase	perimeter subjects and suppliers		If the malfunction cannot be resolved within the time limit, notice is given to end the test execution phase.
DPR 54 art. 7 c. 6	CVCN or CV or LAP	Test report	A test report should be prepared detailing the test environment, tests performed and outcomes	(CVCN the appointee was the LAP).		A test report is prepared detailing the test environment, tests performed and outcomes.
DPR 54 art. 8 c. 1	CVCN or CV	Evaluation report	Within 60 days of the perimeter entity's notification of making the evaluation object available, an appropriate evaluation report shall be prepared and communicated to the perimeter entity and the supplier	perimeter subjects and suppliers		After receiving the perimeter entity's notification of the availability of the evaluation object, an evaluation report is prepared within 60 days.
DPR 54 art. 8 c. 1-3	CVCN or CV	Notification of the final decision of the evaluation process	Within 60 days after the perimeter entity's notice of making the evaluation object available, a reasoned final measure must be communicated to the perimeter entity and the supplier. If the measure is positive, however, prescriptions may be imposed for the use of the object of reliance	perimeter subjects and suppliers		After receiving the perimeter entity's notification of the availability of the evaluation object, a conclusion on the final measures is communicated within 60 days to the supplier and the perimeter entity.

DPR 54 art. 15 c. 2	ACN and specialized facilities of the police and armed forces	Establishing and updating the list of personnel for inspection and verification activities	A list of personnel to be appointed for inspection and verification activities is established and updated. The personnel must meet the requirements of Article 42 l. 124 of 2007 to be able to handle information with security classification higher than "confidential"			A list of personnel to be appointed for inspection and verification activities is defined and updated.
DPR 54 art. 15 c. 3-4	ACN and specialized facilities of the police and armed forces	Identification of personnel in charge	Personnel in charge of audits and inspections are identified, together with a person in charge of the process, according to criteria of professionalism and rotation. Personnel declare the absence of conflict of interest when accepting the assignment	staff in charge		According to the criteria of rotation and professionalism, personnel in charge of audits and inspections are identified. A declaration of absence of conflict is made by the personnel when accepting the assignment
DPR 54 Art. 16 c. 3, DPR 54 Art. 16 c. 5-6 and DPR 54 Art. 18 c. 3	ACN and specialized facilities of the police and armed forces	Notice of initiation of verification and inspection proceedings	The person in charge of the proceedings must notify the persons to whom the proceedings are addressed and those to whom the proceedings may cause prejudice (Art. 7 l. 241 of 1990) of the commencement of the proceedings, in the manner set forth in Art. 8 of l. 241 of 1990. The inspection process must be concluded within one hundred and twenty days from the date of the notice. The inspection process must conclude within ninety days from the date of communication. No less than fifteen days' notice must be given regarding the inspection process. A notice must also be provided, with at least the following information: a) the dates and sites where the inspection will be conducted; b) the persons to be interviewed or their roles and responsibilities; c) the networks, information systems, and information technology services to be inspected; (d) the names of assigned personnel; (e) any other information relevant to the inspection.	Perimeter subjects and any counterinterested parties		The inspection process is concluded within 120 days from the date of the notice. The notification of an upcoming inspection process must be given at least 15 days before the procedure itself, that must be concluded within 90 days from the date of communication. Dates and sites where the inspection will be conducted must be told in the notification. In said notification, the person intervied, their roles and responsabilities, what services and technologies will be inspected, the names of the assigned personnel and any other information relevant for the inspection must also be known.
DPR 54 art. 17 c. 2	perimeter subject	Making available the necessary information and documentation	Following the notice of the initiation of the verification or inspection procedure by the person in charge of the procedure, the perimeter entities shall make available the necessary information and documentation within fifteen days of the request	ACN and specialized facilities of the police and armed forces		In case of request by the person in charge of the procedure, all the necessary information and documentation are make avilable within 15 days of the request.
DPR 54 art. 17 c. 3	perimeter subject	Return of clarifications and additions	Following the request by the person in charge of the procedure, the perimeter parties must respond to requests for clarifications and additions within ten days of the request	ACN and specialized facilities of the police and armed forces		If a request is made by the person in charge of the procedure, the perimeter parties respond for clarifications and additions within 10 days of the request.
DPR 54 art. 16 c. 4 and DPR 54 art. 18 c. 6	perimeter subject	Appointment of a person in charge of the process	Following notice of the initiation of the verification or inspection procedure by the responsible party, perimeter entities must appoint an appointee who possesses professionalism and expertise in cybersecurity. The name of the appointee must be communicated at least five days before the scheduled inspection date.	ACN and specialized facilities of the police and armed forces		An appointee who possesses professionalism and expertise in cybersecurity is appointed by the perimeter entities, following notice of the initiation of the verification or inspection procedure by the responsible party. The name of the appointee is communicated at least 5 days before the scheduled inspection date.
DPR 54 art. 17 c. 4-5 and DPR 54 art. 16 c. 7	ACN and specialized facilities of the police and armed forces	Formation of the record of verification activities	Minutes shall be drawn up of the activity carried out in the course of the checks, which the staff in charge shall forward to the person in charge of the proceedings. If evidence is found of which may constitute violations of regulatory provisions falling within the institutional attributions of other Administrations, the staff in charge shall account for it in the report, and the competent authority shall forward the relevant documentation to the competent Administrations without delay. Specific prescriptions may be formulated with which perimeter parties must comply.	ACN and specialized structures of the Police and Armed Forces (in the figure of the person in charge of the proceedings) and competent administrations with respect to the violation of other regulatory provisions (if they have been detected)		If evidence is found of which may constitute violations of regulatory provisions falling within the institutional attributions of other Administrations, the staff in charge account for it in the report, and the competent authority forward the relevant documentation to the competent Administrations without delay.
DPR 54 art. 18 c. 4-5	perimeter subject	Acceptance or counterproposal to inspection dates	The perimeter subject may accept the proposed dates for the inspection or propose other dates, with a maximum postponement of ten days. In the absence of a counterproposal, the dates are considered confirmed.	ACN and specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)		In proposing new dates for the inspection a maximum of 10 days delay is proposed by the subject. If no counter request is done, then the dates for the inspection are considered accepted.
DPR 54 art. 18 c. 4	ACN and specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)	Acceptance or counterproposal to inspection dates	Upon receipt of the counterproposal for the new dates, the inspection authority shall either accept it or make a counterproposal by sending a notice at least seven days before the scheduled inspection date	perimeter subject		-
DPR 54 art. 18 c. 7	perimeter subject	Making staff available during the inspection	During the inspection, all human resources required and necessary to facilitate related activities should be made available. Access to premises, devices and information relevant to the inspection should be provided.	ACN and specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)		During the inspection, all human resources required and necessary to facilitate related activities are made available and access to premises, devices and information relevant to the inspection is provided.
DPR 54 art. 18 c. 9-10	ACN and specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)	Formation of the record of verification activities	Minutes shall be taken of the activity carried out during the inspection, which the staff in charge shall forward to the person in charge. A copy of the minutes shall be issued to the person in charge of the perimeter subject. If evidence is found of which may constitute violations of regulatory provisions falling within the institutional powers of other Administrations, the assigned personnel shall account for it in the minutes, and the competent authority shall forward the relevant documentation to the competent Administrations without delay.	ACN and specialized facilities of the Police and Armed Forces (in the figure of the person in charge of the proceedings), perimeter subjects (in the figure of the person in charge), and competent administrations with respect to the violation of other regulatory provisions (when detected)		If evidence is found of which may constitute violations of regulatory provisions falling within the institutional powers of other Administrations, the assigned personnel account for it in the minutes, and the competent authority forward the relevant documentation to the competent Administrations without delay.
DPR 54 art. 19	ACN and specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)	Outcomes of inspection or verification activities	An order concluding the proceedings should be adopted, imparting specific requirements if necessary. The measure must be communicated to the person concerned. Where necessary, proceedings for the application of sanctions shall be initiated.	perimeter subjects		An order for the conclusion of the proceedings is adopted and the measures are communicated to the person concerned before initiating the proceeding for the application of sanctions .
D.P.C.M. 15 June 2021	perimeter subject	Extension of obligation provided by DPR 54 to a) hardware and software components that perform telecommunications network functions and services (access, transport, switching); b) hardware and software components that perform functions for the security of telecommunications networks and the data they process; c) hardware and software components for data acquisition, monitoring, supervision, control, implementation and automation of telecommunications networks and industrial and infrastructure systems; d) software applications for the implementation of security mechanisms.				
D.P.C.M. 18 maggio 2022, n. 92, art. 4	CVCN	The CVCN: a) accredits the testing laboratories, in possession of the requirements; b) undertakes initiatives in order to guarantee the maintenance of the quality level of the LAPs and the correct implementation of the technical determinations, the technical specifications and the drawing up of the test reports; c) establishes the test methodologies; d) supervises the activity of the LAPs; e) adopts specific technical determinations, ensuring, within its own competences, their compliance and taking care of their updating f) supervise the connections with the LAPs and the VCs, also in order to ensure the coordination of their respective activities and to pursue the convergence and non-duplication of assessments in the presence of the same conditions and risk levels; g) draw up and periodically update the list of ICT goods, systems and services subject to assessment, for which a test report has been issued.				
D.P.C.M. 18 maggio 2022, n. 92, art. 14	CVCN	The CVCN arranges for audits to be carried out periodically, at a maximum of every 18 months, to verify the maintenance of the accreditation requirements. The CVCN may carry out random inspections to verify the fulfilment of the conditions for maintaining accreditation. The CVCN, at least two months in advance of the scheduled date, informs the LAP of the date scheduled for the surveillance inspection, requesting any integration of the documentation in the event of any changes that have resulted in the need to revise the system documentation.				
D.P.C.M. 18 maggio 2022, n. 92, art. 13	LAP	For the purposes of maintaining accreditation, LAPs are obliged to: a) operate on the basis of what is provided for in the technical determinations; b) promptly inform the CVCN of any variation concerning the information submitted in support of the application for accreditation; c) transmit the test report to the CVCN within the established deadlines; d) carry out the activities related to the accreditation exclusively at the premises located on the national territory and indicated in the application for accreditation; e) ensure adequate training of its personnel in order to comply with the non-disclosure commitment; f) inform the CVCN and the eventual LAP has processed data or systems concerning the latter, of any limitation of operations for more than 24 hours, within the following 24 hours.				
GDPR art. 2 c. 1	Companies and private entities	Material scope	This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.			-
GDPR art. 3 c. 1	Companies and private entities	Territorial scope	This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.			-
GDPR art. 3 c. 2a	Companies and private entities	Territorial scope	This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or			-
GDPR art. 3 c. 2b	Companies and private entities	Territorial scope	This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.			-
GDPR art. 3 c. 3	Companies and private entities	Territorial scope	This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.			-

GDPR art. 5 c. 1 a-b-c-d-e-f	Companies and private entities	Applicable principles to personal data processing	Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance			Processes are defined and managed so that personal data are ensured to be processed in compliance with the principles of lawfulness, correctness, transparency, purpose limitation, data minimization, accuracy, retention limitation, integrity and confidentiality. Compliance with the Regulation is demonstrated through the preparation of a Personal Data Processing Register which allows, for example, the mapping of the flows of personal data processed, the definition by design and by default of protocols for the application of the principles.
GDPR art 24 c. 1	Companies and private entities	Responsibility of the data controller	Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.			Adequate personal data protection policies are defined and implemented. The technical measures adopted are reviewed and updated as necessary.
GDPR art 25 c. 1	Companies and private entities	Data protection by design & data protection by default	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.			The controller implements appropriate technical and organizational measures to effectively implement data protection principles (e.g. pseudonymisation, minimisation) by design (data protection by design). The data controller implements appropriate technical and organizational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed, by default (data protection by default).
GDPR art 25 c. 2	Companies and private entities	Data protection by design & data protection by default	The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.			Appropriate technical and organizational measures are implemented by the data controlle to effectively implement data protection principles (e.g. pseudonymisation, minimisation) by design (data protection by design). Appropriate technical and organizational measures are implemented by the data controller to ensure that only the personal data necessary for each specific purpose of the processing are processed, by default (data protection by default).
GDPR art 25 c. 3	Companies and private entities	Data protection by design & data protection by default	An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.			The controller implements appropriate technical and organizational measures to effectively implement data protection principles (e.g. pseudonymisation, minimisation) by design (data protection by design). The data controller implements appropriate technical and organizational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed, by default (data protection by default).
GDPR art 32 c. 1 a-b-c-d	Companies and private entities	Security of processing	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.			Adequate technical and organizational measures are adopted to guarantee a level of security appropriate to the risk through, for example, the periodic planning of audit activities, the periodic carrying out of assessments regarding the risks deriving from the processing of personal data, the adoption of internal procedures and/or codes of conduct aimed at ensuring effective compliance with the principles set by the GDPR.
GDPR art 32 c. 2	Companies and private entities	Security of processing	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.			The appropriate level of security is assessed taking into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
GDPR art 32 c. 3	Companies and private entities	Security of processing	Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.			-
GDPR art 32 c. 4	Companies and private entities	Security of processing	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.			Adequate technical and organizational measures are adopted to guarantee that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law
GDPR art 35 c. 1	Companies and private entities	Data protection impact assessment	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.			An impact assessment on the protection of personal data is carried out, containing the provisions of the Regulation. That impact assessment is subject to periodic re-evaluation.
GDPR art 35 c. 2	Companies and private entities	Data protection impact assessment	2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.			The Dpo, if appointed, is involved in carrying out a data protection impact assessment.
GDPR art 35 c. 3 a-b-c	Companies and private entities	Data protection impact assessment	A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.			A periodic impact assessment must is persued whenever there is a case compelling: (a) processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; (c) a systematic monitoring of a publicly accessible area on a large scale.
GDPR art 35 c. 4	Companies and private entities	Data protection impact assessment	4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.			The list regarding the kind of processing operations carried out and subjects to the requirement for a data protection impact assessment pursuant to Article 35(1) is made public and communicate to the Board referred to in Article 68.
GDPR art 35 c. 5	Companies and private entities	Data protection impact assessment	5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.			The list of processing operations for which data protection is not is communicated to the board by supervisory authorities.
GDPR art 35 c. 6	Companies and private entities	Data protection impact assessment	6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.			An adequate consistency mechanism (referred in article 63) was put in place before the adoption of the lists referred to in pragraph 4 and 5 everytime suchs lists involve processing activities related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
GDPR art 35 c. 7 a-b-c-d	Companies and private entities	Data protection impact assessment	7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.			A data protection impact assessment is carried out containing: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

GDPR art 35 c. 8-9-10-11	Companies and private entities	Data protection impact assessment	8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. 10. Where processing pursuant to point (c) or (e) of Article 6 (1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities. 11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.			8. Controllers or processors take into due account the ompliance with approved codes of conduct referred to in Article 40 while assessing the impact of processing operations performed by such controllers or processors, in particular for the case of data protection impact assessment; 9. The controller shall not projudice the security of commercial or public interests or the security of processing while he seeks views of data subjects or their representative; 11. Everytime there is a change on the risk represented a review of the assessment is carried aout to assess if processing is performed in accordance with the data protection impact assessment.
GDPR art 64 c. 1 a	Companies and private entities	Opinion of the board	1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it: (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);			Opinions are exchanged between the Board and supervisory authorithies everytime the supervisory authority intends to adopt any of the measures defined in Article 64(1) and communicate to the board the draft decision.