COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Italy

DATA PROTECTION & CYBERSECURITY

Contributor

ICT Legal Consulting

Paolo Balboni

Founding Partner | paolo.balboni@ictlc.com

Luca Bolognini

Founding Partner | luca.bolognini@ictlc.com

Francesco Capparelli

Chief Cyber Security Advisor | francesco.capparelli@ictlc.com

Isabella Oldani

Senior Associate | isabella.oldani@ictlc.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Italy.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

ITALY
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Italian legislative approach to data protection and cybersecurity is characterised by the harmonious integration of EU directives and national regulations, creating a detailed and comprehensive system to ensure data protection and enhance cyber resilience.

The main laws governing privacy and data protection in Italy are as follows:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, known as the "General Data Protection Regulation" or "GDPR";
- Legislative Decree No. 196/2003 ("Privacy Code"), as amended by Legislative Decree No. 101/2018 and, most recently, by Law Decree No. 139/2021, converted, with amendments, by Law No. 205/2021 and Law Decree No. 132/2021, converted, with amendments, by Law No. 178/2021. These amendments harmonise the Italian data protection framework with the GDPR and transpose Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (known as the "e-Privacy Directive");
- Legislative Decree No. 51/2018, which transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (known as the "Police Directive") into the Italian legal framework.

The Privacy Code designates the *Garante per la protezione dei dati personali* (GPDP) as the supervisory authority in Italy responsible for monitoring compliance with data protection legislation.

With regard to the Italian legal framework on cybersecurity, the main legal acts include:

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on the certification of the cybersecurity of information and communication technologies ("Cybersecurity Act");
- Legislative Decree No. 65/2018, which transposes Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 (the "NIS Directive") into the Italian legal framework;
- Legislative Decree No. 105/2019, establishing the National Cybersecurity Perimeter (*Perimetro di Sicurezza Nazionale Cibernetica* – "PSNC");
- Prime Ministerial Decree (DPCM) No. 131/2020, the "Regulation on the National Cybersecurity Perimeter";
- Legislative Decree No. 82/2021, containing "Urgent provisions on cybersecurity, the definition of the national cybersecurity architecture and the establishment of the National Cybersecurity Agency" (*Agenzia per la Cybersicurezza Nazionale* – "ACN").

Strengthening the cybersecurity framework, 'Directive (EU) 2022/2555', also known as the NIS2 Directive, expands the scope originally established by its predecessor, the NIS Directive, which was incorporated into the Italian legal system by Legislative Decree No. 65/2018. This updated Directive, which Member States are required to transpose into national law by 17 October 2024, reinforces cybersecurity protocols in various sectors such as energy, transport, banking and digital infrastructure, thereby contributing to the security and resilience of critical services.

In synergy with the NIS2 Directive is the Digital

Operational Resilience Act (DORA), a key piece of legislation aimed at strengthening digital operational resilience in the European Union's financial sector. Following its approval by the European Parliament on 10 November 2022, it entered into force on 16 January 2023 and will become binding on 17 January 2025. DORA establishes a framework to ensure that financial institutions, which include banks, insurance companies and cryptocurrency service providers, maintain robust digital operational resilience, thereby safeguarding financial stability in the current scenario of an increasingly digitised landscape.

Complementing this regulatory framework is Regulation (EU) 910/2014, known as the eIDAS Regulation, which regulates electronic identification and trust services.

The European Commission has published two draft regulations for an initiative known as the Cyber Resilience Act (CRA). This act aims to ensure that digital products placed on the European market comply with robust cybersecurity standards, thereby establishing a significant level of responsibility on the part of manufacturers. In the second half of 2023, a preliminary agreement was reached on the Cyber Resilience Act. The Act is expected to be put to a vote during the plenary session of the Parliament in April 2024.

A new bill in Italy, aimed at strengthening national cybersecurity and combating cybercrime, was approved by the Council of Ministers on 25 January 2024 and submitted to the legislative bodies on 16 February 2024. This legislative initiative represents a significant step forward in refining Italy's approach to cybersecurity and cybercrime. With this bill, Italy seeks to enhance its national digital security framework with specific, targeted measures, demonstrating a holistic approach to the prevention and effective management of cyber incidents.

As for the authorities that are in charge of overseeing compliance with cybersecurity requirements, please see question 33.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

The landscape of data protection, privacy, and cybersecurity is poised for significant evolution in the years 2024 and 2025, with a series of anticipated developments shaping the future of how personal and corporate data is managed and protected.

In the United States, the introduction of new state-level data privacy laws is on the horizon, with several states poised to adopt regulations akin to those already in place in California and Virginia. These forthcoming statutes are expected to empower consumers with greater control over their personal information, granting them the rights to access, amend, and delete their data, alongside the ability to opt-out of the sale of their personal information.

Across the Atlantic, the European Union's Data Act, which officially took effect in January 2024, is another landmark piece of legislation set to influence the digital landscape. Although its full obligations will not be mandatory until September 12, 2025, the act is designed to foster innovation and consumer empowerment in the realm of connected devices, all while safeguarding trade secrets.

Enforcement of existing regulations is also anticipated to intensify, with regulatory bodies, especially within the European Union under the General Data Protection Regulation (GDPR), expected to heighten their oversight of data brokerage, the utilization of biometric data, the handling of children's data, and the deployment of Artificial Intelligence (AI) technologies.

The dialogue surrounding potential amendments and new regulations is equally dynamic. In the United States, discussions regarding a comprehensive federal data privacy law continue to unfold. Although its enactment in 2024 remains uncertain, the progression of this debate warrants close observation. Meanwhile, the United Kingdom is deliberating modifications to its data protection framework through the Data Protection and Digital Information Bill, with conclusions anticipated by 2025.

A defining characteristic of this evolving terrain is the increasing fragmentation of global data protection standards. As jurisdictions worldwide implement their own distinct legal frameworks, the complexity for businesses operating across borders escalates. Organizations will need to navigate this patchwork of regulations with caution, ensuring their data processing activities comply with the varying requirements imposed by different laws and regulations. This trend underscores the importance of adaptability and vigilance in the face of an ever-changing regulatory environment, highlighting the need for companies to stay informed and agile in their data protection strategies.

From a cybersecurity perspective, the inception of the Digital Operational Resilience Act (DORA) and the

second Network and Information Systems Directive (NIS2) in the years 2024 and 2025 heralds a significant turning point in the field of cybersecurity, especially within the European context. These regulatory milestones are not just mere additions to the existing legislative framework; they represent a concerted effort by the European Union to elevate the standards of cybersecurity and operational resilience across diverse sectors. This initiative reflects a deep-seated commitment to reinforcing the digital defenses of the European bloc.

With their enactment in late 2022, DORA and NIS2 embody the European Union's forward-thinking strategy to confront the burgeoning cyber threats of our time. They aim to foster a cohesive cybersecurity stance among the member states, thereby ensuring a united front against potential digital vulnerabilities. NIS2, in particular, broadens its horizon beyond its predecessor's boundaries, embracing an extensive array of critical and significant entities within vital sectors like energy, transport, banking, digital platforms, and healthcare. Its mission is to buttress the cybersecurity frameworks of these sectors to withstand the dynamic landscape of cyber threats.

DORA, with its laser focus on the financial sector, introduces rigorous standards for cybersecurity and operational resilience. This regulation mandates banks, investment firms, insurance entities, and other financial institutions to uphold a formidable defense against operational disturbances, catering specifically to the nuanced demands of the financial industry. When the jurisdictions of DORA and NIS2 overlap, the former takes precedence, emphasizing its pivotal role in safeguarding the financial sector's integrity.

As these regulations unfurl their full potential, they bring about a paradigm shift in compliance expectations. Organizations within their scope are now tasked with adopting more stringent cybersecurity measures, a holistic approach to risk management, and an unambiguous protocol for incident reporting. A significant emphasis is placed on the security of supply chains, urging entities to meticulously scrutinize and mitigate risks introduced by external vendors and service providers.

The European Union's stringent enforcement stance and the prospect of severe penalties underscore the critical nature of these directives. This serves as a clarion call to entities to align their operations with these regulations to avert financial repercussions and protect their reputational capital.

The strategic unveiling of DORA and NIS2 marks a proactive step by the European Union towards fortifying its digital infrastructure. As these directives become fully operational, they compel a reevaluation of cybersecurity strategies among businesses, particularly those within the critical infrastructure and financial sectors. This adaptation is crucial for navigating the ever-evolving regulatory landscape and achieving compliance, underscoring a broader global movement towards the fortification of digital security frameworks.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

Under the framework of the GDPR and the Italian Privacy Code, entities subject to data protection and privacy laws are not obliged to undergo any registration or licensing requirements. This approach stems from the overarching principle of accountability, which gives data controllers considerable autonomy in managing their operational and organisational practices. However, organisations that designate a data protection officer (DPO) in accordance with the requirements of the GDPR are required to submit the DPO's contact information to the GPDP through an online procedure provided by the latter. In addition, there are provisions under which organisations may be required to consult with the GPDP, which are discussed in the following sections.

In addition, the Italian government, through ACN Resolution No. 307/2022, has issued a regulation on the accreditation of cloud services used by public administrations, with the aim of raising cybersecurity standards. According to this regulation, cloud service providers are required to undergo a comprehensive verification of their highest security measures. In particular, they must obtain a specific qualification from the ACN to process data, with the qualification criteria varying depending on the type of data handled. ACN has extended the end of the transitional regime for the qualification of cloud infrastructures and services for public administrations until 30 June 2024.

For ACN accreditation, cloud services are expected to have ISO 9001 certification along with ISO/IEC 27001 or alternatively CSA-Star Level 2 certification. They are required to demonstrate the existence of robust quality and information security management systems, which are essential for protecting customer data and information. Such certifications are critical to ensuring that cloud service providers adhere to stringent standards, thereby supporting a secure and reliable cloud services infrastructure.

4. How do these data protection laws define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”) versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

The definitions of “personal data” and “special categories of personal data” are set forth under the GDPR. According to art. 4.1 GDPR, personal data is defined as “*any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*”. Special categories of personal data are those identified by art. 9.1 GDPR and, precisely, “*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation*”. The GDPR also contemplates, in art. 10 GDPR, the category of personal data relating to criminal convictions and offences.

The definition of personal data, as described above, extends its relevance to cybersecurity, however, cybersecurity legislation encompasses a wider range of information beyond the scope of the GDPR and includes all forms of data, including non-personal and business-related data.

Non-personal data is categorised into two types based on its origin: firstly, data that is inherently unrelated to an identified or identifiable individual, such as meteorological data from sensors on wind turbines or operational data from industrial machinery; and secondly, data that was initially classified as personal but has subsequently been anonymised, thereby losing its identifiable characteristics.

The term “business data” refers to the variety of information generated, collected, processed and stored by an organisation in the course of its business activities.

In addition, ACN Resolution No. 307/2022 outlines a systematic framework for classifying government data into three distinct levels: ordinary, critical and strategic. This classification aims to strengthen data security through a comprehensive set of criteria that address key security areas, including asset management, governance, risk assessment, supply chain security, identity management, data backup, protective procedures and protocols, information retention and industrial control systems, and the use of technical security measures. Data classification is essential to determine the necessary safeguards for each category of data, thereby maintaining the integrity, confidentiality and availability of such data. Effective data classification enables public sector organisations to enhance their data protection strategies, mitigate cybersecurity risks, and implement tailored security protocols and policies to protect sensitive data. Such careful data management helps to strengthen the security and resilience of government infrastructures.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or “fair information practice principles” in detail.

The general principles applicable to the processing of personal data are set out in the GDPR and include the following:

- Principle of lawfulness (Art. 5.1.a) GDPR) – The processing of personal data must have a legal basis according to the GDPR;
- Principle of fairness (Art. 5.1.a) GDPR) – The processing of personal data must be based on the principles of honesty and good faith;
- Principle of transparency (Art. 5.1.a), 12, 13 and 14 GDPR) – Data subjects shall be adequately informed of the processing activities carried out in relation to their personal data;
- Principle of purpose limitation (Art. 5.1.b) GDPR) – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- Principle of minimisation (Art. 5.1.c) GDPR) – Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Principle of Accuracy (Art. 5.1.d) GDPR) – Personal data must be accurate and, where

necessary, updated;
- Principle of storage limitation (Art. 5.1.e) GDPR) – Personal data shall be 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;
- Principle of integrity and confidentiality (Art. 5.1.f) and 32 GDPR) – Appropriate security measures shall be implemented to protect personal data from certain adverse events (including unauthorised or unlawful processing, accidental loss, destruction or damage);
- Principle of accountability (Article 5.2 GDPR) – The data controller must ensure compliance with these principles and be able to demonstrate such compliance.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Yes, consent is required by law in certain cases, such as direct marketing activities using automated calling systems without human intervention, fax, e-mail, SMS, MMS and other similar technologies, as described in Articles 130.1 and 130.2 of the Privacy Code. In addition, consent is required for the storage of or access to information on the terminal equipment of the contracting party or user, as provided for in article 122 of the Privacy Code. Furthermore, the GPDP provides for consent in certain situations through its rulings, including, but not limited to, the processing of genetic data for specific purposes.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

According to Article 4(11) of the GDPR, consent is only considered valid if it is freely given, specific, informed and unambiguous. This requirement is fundamental to the GDPR's approach to data protection, ensuring that individuals are fully aware of, and consent to, the processing of their data. In addition, for the processing of special categories of personal data, the GDPR stipulates in Article 9(1) that consent must not only meet the general standards, but must also be explicit. This heightened requirement highlights the importance of clear and informed consent when dealing with sensitive data, ensuring that such information is processed with the utmost care and explicit permission.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

In general, the GDPR prohibits the processing of special categories of data, as set out in Article 9(1). This prohibition applies unless certain exceptions apply, as set out in Article 9(2) of the GDPR. One notable exception is the explicit consent of the data subject. In addition, Article 9(4) of the GDPR allows Member States to impose additional conditions, safeguards and provisions to monitor the processing of sensitive data, including genetic, biometric or health data. This provision is mirrored in Article 2-septies of the Italian Privacy Code, which is referred to in question 10 below for further details. It's important to note that there are no categories of personal data or personally identifiable information (PII) that are categorically prohibited from being collected under the GDPR, provided that the relevant legal basis or exceptions are met.

9. How do the data protection laws in your jurisdiction address health data?

The processing and protection of health data is subject to strict regulations under the General Data Protection Regulation (GDPR), and is specifically identified as "special categories of personal data" under Article 9. This classification highlights the sensitive nature of health data, which requires the explicit consent of the data subject or a legitimate need for medical treatment to justify its processing. In addition, the Italian Privacy Code requires compliance with specific protection measures for the handling of health data, as outlined by the Italian Data Protection Authority (Garante per la protezione dei dati personali, GPDP) every two years under Article 2-septies. This includes a prohibition on the wide dissemination of health, genetic and biometric data, further emphasising the need for confidentiality and privacy.

Article 2-sexies sets out the circumstances in which the processing of such sensitive data is considered necessary for tasks in the public interest, thus delineating the careful balance between individual privacy rights and societal benefits. A notable

clarification by the GPDP in March 2019, referring to GDPR Articles 9.2(h) and 9.3, exempts healthcare professionals bound by confidentiality from requiring patient consent for data processing related to the provision of healthcare. However, any processing beyond this scope requires the explicit consent of the patient.

In addition, the Italian Law No. 833/1978, which establishes the National Health Service, lays down comprehensive rules for the management of health data in the health sector. This law outlines the responsibilities of healthcare providers and sets criteria for the collection, storage and use of health information. It also covers the implementation and use of the electronic health record system (Fascicolo Sanitario Elettronico) and prescribes specific measures for the management of health data within this framework. The GPDP has also issued guidelines on the Electronic Health Record (Dossier Sanitario Elettronico) – detailing the handling of medical histories within healthcare facilities – and on protocols for online medical reports, which include clinical or instrumental examination results issued by medical professionals.

Moreover, the EU's Medical Devices Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR) provide a regulatory framework for the safety, design, manufacture and use of medical devices. These regulations aim to ensure the highest level of protection of health data and safety of medical devices, reflecting the critical intersection of privacy, health and technology in the healthcare sector.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Beyond the general principles regarding the handling of personal data under the GDPR and the Italian Privacy Code, there are specific provisions that allow for exceptions, exclusions or limitations to these rules, particularly in contexts that serve broader societal interests. These provisions take into account the nuanced balance between individual data protection rights and the imperative of serving the public interest, facilitating scientific development, or upholding freedom of expression and information.

A key area of divergence relates to the processing of personal data for archiving in the public interest, scientific, historical research or statistical purposes. The Privacy Code recognises the critical value of preserving such data for future generations, advancing knowledge and informing public policy. Such processing activities are subject to conditions and safeguards to ensure respect for the fundamental rights and freedoms of data subjects, reflecting a tailored approach to data protection that takes into account the specificities and benefits of research and archiving activities.

In addition, the Privacy Code recognises the essential role of journalism in a democratic society. It provides for specific exceptions in the context of journalistic activities to ensure that data protection does not impede freedom of the press and the public's right to information. These provisions underline the importance of balancing privacy rights with freedom of expression and the societal need for investigative journalism.

The Privacy Code also introduces limitations on the rights of data subjects in certain contexts. For example, Article 2 provides that the rights granted to data subjects under Articles 15-22 and 77 of the GDPR may not be invoked in situations where the exercise of those rights would significantly harm protected interests, such as the confidentiality of whistleblowers' identities or the integrity of anti-money laundering measures. This recognises the complex interplay between individual rights and collective interests and ensures that data protection does not inadvertently compromise important societal values.

Furthermore, Article 2-duodecies allows for the modification or suspension of certain GDPR rights and obligations (Articles 12-22 and 34) in the area of judicial proceedings. This provision recognises the unique requirements of judicial systems, allowing certain data protection measures to be adapted or suspended to ensure the proper administration of justice. This includes delaying or limiting the rights of data subjects so as not to interfere with judicial proceedings, underlining the careful balance between the protection of personal data and the operational needs of the justice system.

These exceptions, exclusions and limitations illustrate the flexible and pragmatic approach to data protection of the GDPR and the Italian Privacy Code, which recognises that the strict application of data protection rules is not always compatible with other public interest considerations or the need for freedom of expression and information.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Given the acute awareness of the increased vulnerability

of this age group and the need for enhanced safeguards, data protection legislation in European and Italian jurisdictions explicitly addresses the processing of personal data of children and teenagers.

The General Data Protection Regulation (GDPR), in its Article 8(1), sets out specific provisions regarding the age at which minors can independently consent to the processing of their personal data for information society services. This age is set at 14 years. For children under this age, the law requires that the consent of their parents or legal guardians be obtained, thus creating a protective barrier against unauthorised data processing.

However, the law also allows for certain exceptions to this rule. In certain circumstances, children under the age of 14 may give their consent directly, if this is provided for in specific legislation. In addition, data controllers may collect and use the data of minors without obtaining consent in situations where such processing is necessary for the protection of the child.

Data controllers are subject to a number of strict obligations aimed at strengthening the protection of minors' personal data. These obligations include the implementation of appropriate technical and organisational measures to ensure data security, the provision of clear and comprehensible information to both minors and their guardians about the risks and procedures involved in data processing, and the need to obtain consent in an unambiguous, informed and explicit manner.

To further protect minors' data, several security measures are recommended, such as the pseudonymisation and anonymisation of personal data, the restriction of access to data to authorised persons, the implementation of strict controls on the use of data, and the provision of simple mechanisms for the deletion of data.

The Italian Data Protection Authority (Garante per la protezione dei dati personali), which acts as the supervisory authority, oversees the enforcement of these rules. It also disseminates specific guidelines and resources on the protection of personal data of children and teenagers through its official web platform.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The Italian data protection framework addresses online safety to the extent that certain behaviours online would amount to the infringement of data protection rules and principles. In addition to this and besides the provisions set out under the Digital Services Act that applies across the EU, it should be noted that some additional pieces of legislation have been specifically adopted in Italy for the purpose of contributing to the creation of a safer digital space.

In particular, it is worth noting that **Law no. 71/2017** on the "Regulation for the safeguarding of minors and the prevention and tackling of **cyberbullying**" plays a crucial role in protecting minors online, in that it makes illegal whatever form of psychological pressure, aggression, defamation, identify theft (and other conducts identified under the definition of "cyberbullying") of personal data of minors and / or their dissemination through electronic means.

In addition to the above, besides provisions on general offenses concerning violence, it is also worth mentioning that the Italian Criminal Code envisages under Article 612-bis the specific offence on **stalking**. The same Article also specifies that the fact that ICT tools are used is an aggravating circumstance of the offense. The Italian Criminal Code also punishes, under Article 612-ter, the so-called offense of "**revenge porn**", which consists in the unlawful distribution of sexually explicit images or videos without the consent of the individuals represented in that content. The penalty envisaged for this offense (imprisonment from one to six years and a fine from € 5000.00 to€15.000.00) also applies to those who further distribute those images or videos that they have received or otherwise acquired for the purpose of harming the individuals concerned.

Some additional safeguards are also provided under Article 7-bis of Law Decree No. 28/2020 entitled "Systems for the protection of minors from the risks of cyberspace". The said Article sets out specific obligations for electronic communication service providers with respect to the filtering of explicit content that is delivered by means of their services so as to limit minor's exposure to content that may be harmful for their growth and personality. This provision sets out, among others, the obligation for electronic communication service providers to implement parental control measures for filtering inappropriate content for minors.

Additional provisions aimed at protecting consumers and minors from inappropriate content are also included in the national legislation that transposes within the Italian legal framework requirements set out under EU acts, such as the Audiovisual Media Services Directive (transposed within the Italian legal framework by means

of Legislative Decree no. 208/2021). Some additional and more specific bans are also included in the so-called the "Dignity Decree" (effective July 14, 2018) in relation to the advertising of gambling products and services (including by means of cyber, digital and other electronic means) for the purpose of protecting "vulnerable" categories (such as gambling addicts as well as minors).

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

The Italian legal frameworks entrusts the Italian Data Protection Authority with specific enforcement powers in relation to actions that amount to a form of "cyberbullying" or "revenge porn". In particular, Law no. 71/2017 on the "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying" provides that underage victims that are at least 14 years old (or their parent) can contact the data controller / website or social media provider in order to request for the blocking / removal of personal data pertaining to the victim. In case the request is not fulfilled after 48 hours, a claim can be lodged to the Italian Data Protection Authority which (within 48 hours of receiving the claim) will take actions pursuant to Articles 143 and 144 of the Italian Data Protection Code (Article 144 provides that the Italian Data Protection Authority will take any claims received into consideration for the purpose of exercising its enforcement powers pursuant to Article 58 of the GDPR).

Likewise, as for conducts that allegedly amount to a form of "revenge porn", Article 144-bis of the Italian Data Protection Code provides that, in case individuals fear that sexually explicitly images have been disseminated without their consent, they can submit a report to the Italian Data Protection Authority which will adopt (where appropriate) the measures that it will deem necessary in order to counter such dissemination.

The enforcement powers attributed to the Italian Data Protection Authority are also supplemented by those attributed to the Italian Postal and Communication Police and the criminal enforcement system more broadly to which similar actions can also be reported in the event that a given behaviour presents elements potentially relevant under the criminal legal system. In order to strengthen their respective actions against "cyberbullying", it is worth recalling that the Italian Data Protection Authority has entered into a Memorandum of Understanding with the Italian Postal and Communication Police. Pursuant to the said Memorandum of Understanding, both bodies commit to cooperate for the purpose of identifying the relevant data controller / website or social media provider (where the illicit content has been disclosed) and for the purpose of implementing the necessary actions as a remedy for the affected minors. A specific duty of cooperation is also envisaged under Article 144-bis of the Italian Data Protection Code which provides that, where the Italian Data Protection Authority "*becomes aware of the commission, including attempted commission, of the criminal offence referred to*" in Article 612-ter of the Criminal Code, "*it shall forward the said report and any documents it has acquired to the public prosecutor if the offence at issue may be prosecuted ex officio*".

Some specific enforcement powers are also entrusted to the Italian Communications Authority (*Autorità per le garanzie nelle comunicazioni*, AGCOM), which (among others) shall order the relevant providers to bring to an end the violation of the provision set out under the abovementioned Article 7-bis of Law Decree No. 28/2020. It is also worth noting that the EU Commission has signed an administrative arrangement with the same authority (the Italian Communications Authority) in order to support the EU Commission's supervisory and enforcement powers under the Digital Services Act. Moreover, a specific cooperation has been established between the Italian Data Protection Authority and the Italian Communications Authority in 2023 for the purpose of strengthening the protection of minors by promoting the creation of age verification systems (as a condition for accessing online services) and by experimenting new forms of cooperation between the two authorities (e.g., exchanging of information, launching of public consultations).

For the same of completeness, it is worth mentioning that certain advertising activities may also fall under the competence of the Italian Competition Authority (*Autorità della Concorrenza e del Mercato*).

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

2024 – 2025 will mark the first year of implementation of the Digital Services Act, which would give the opportunity to assess its impact in creating a secure and trusted online environment in Italy and across the EU more broadly.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

The principles of "data protection by design" and "data protection by default" are fundamental elements of the GDPR, which applies to any organisation operating in the EU or handling the personal data of individuals residing in the EU. These principles are set out in Article 25 of the GDPR.

Data Protection by Design (Article 25.1 GDPR) mandates that data protection measures must be built into processing activities and the development of products or services from the outset. This means that data controllers (those who determine the purposes and means of processing personal data) must consider privacy and data protection aspects as part of the design and implementation of systems, services and products. A practical approach to achieving this includes the use of Privacy Enhancing Technologies (PETs), minimising the processing of personal data, pseudonymising data as soon as possible, and building secure systems by default.

Data protection by default (Article 25.2 GDPR) requires that, by default, only personal data necessary for each specific purpose of processing is processed. This applies to the amount of personal data collected, the scope of its processing, the period of its storage and its accessibility. Measures must be taken to ensure that personal data are not made available by default to an indefinite number of individuals. This principle emphasises minimising data collection and access, and ensuring that default settings in applications and platforms are privacy-preserving.

To comply with these principles, companies typically adopt several practices:

1. Conducting Data Protection Impact Assessments (DPIAs): While DPIAs are specifically required under Article 35 of the GDPR for processing that is likely to result in a high risk to individuals' rights and freedoms, they are also considered a best practice for implementing privacy by design and default. DPIAs help to identify and mitigate data protection risks in new projects or when introducing new technologies.
2. Adoption of Privacy-Enhancing Technologies (PETs): These are technologies that support the implementation of data protection principles by minimising the use of personal data, maximising data security and giving individuals control over their personal data.
3. Privacy and security measures: Implementing strong encryption, secure data storage and access controls are examples of technical measures. Organisational measures include privacy policies, employee training, and privacy governance structures.
4. Regular Audits and Reviews: Ensuring that data protection measures remain effective and are updated in line with new threats or advances in technology.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Under the GDPR, the principle of accountability is paramount and is articulated in Article 5(2). This principle requires that data controllers are not only responsible for complying with the requirements of the GDPR, but must also be able to actively demonstrate their compliance. This demonstration can take a number of forms, including keeping detailed records, conducting thorough data protection impact assessments (DPIAs) and documenting the reasons for processing decisions, particularly where these are based on the controller's legitimate interests.

A critical component of this accountability framework is the requirement for both controllers and processors to keep comprehensive records of their data processing activities, as set out in Article 30 of the GDPR. These records must include, among other things, the purposes of the processing, the categories of data subjects and personal data processed, the categories of recipients to whom the data has been or will be disclosed, and details of cross-border data transfers. This documentation serves not only as a tool for compliance, but also as a means of demonstrating such compliance to supervisory authorities upon request.

In addition, the GDPR introduces the concept of DPIAs, which are essential for identifying, assessing and mitigating the risks associated with data processing activities, particularly those that pose a high risk to the rights and freedoms of individuals. The DPIA process involves a detailed analysis of the necessity and proportionality of processing activities and includes measures to address and mitigate any identified risks.

This process not only assists in compliance, but also in the strategic planning of data processing activities, ensuring that they are designed with privacy considerations at their core.

Another aspect of demonstrating compliance, particularly where processing is based on legitimate interests (as set out in Recital 47 of the GDPR), is the careful documentation of the balance of interests test. This requires data controllers to conduct a careful assessment of their legitimate interests against the interests, rights and freedoms of data subjects. The results of this assessment must be documented and made available as part of the organisation's compliance records.

To meet these GDPR requirements, organisations typically develop and implement robust data protection policies and procedures that reflect their processing activities and the measures they've put in place to ensure compliance. This also includes regular training and awareness programmes for staff, to embed a culture of data protection within the organisation. For many organisations, the appointment of a Data Protection Officer (DPO) is either a mandatory requirement or best practice, to provide expert guidance and oversight on compliance matters.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Under the General Data Protection Regulation (GDPR), which applies to all member states of the European Union and the wider European Economic Area, data protection laws do indeed require the implementation of data retention and disposal policies and procedures. These requirements are integral to the principles of data minimisation and storage limitation, which are at the heart of the GDPR's approach to privacy and data protection.

- Data retention policies

The GDPR does not prescribe specific retention periods for personal data; instead, it requires that personal data be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This principle, found in Article 5(1)(e), implies a requirement for organisations to establish data retention policies that clearly define how long personal data will be retained before being deleted or anonymised. The data retention period must be justified based on the purpose of the data processing activity, as well as other legal or regulatory requirements that may necessitate longer retention periods (e.g. tax laws, labour laws, etc.).

- Data Disposal Procedures

In the context of data retention, the GDPR also requires secure data disposal procedures to ensure that once the retention period has expired or the data is no longer needed for the original purpose, it is disposed of in a manner that prevents its reconstruction or recovery. Article 5(1)(f) emphasises the need for security of processing, which extends to secure data disposal and ensures that personal data is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

Under the regulatory framework established by the General Data Protection Regulation (GDPR), there are specific circumstances in which data controllers operating within their jurisdiction are either required or encouraged to consult with the relevant Data Protection Authority(ies). This requirement is intended to ensure that data processing activities that pose a high risk to the privacy and protection of personal data are carried out under the guidance of, and with the necessary oversight from, data protection authorities. The scenarios requiring consultation are primarily detailed in Article 36 of the GDPR, as well as in specific national legislation, such as the Italian Privacy Code, which complement and specify the GDPR provisions in certain contexts.

Under Article 36 of the GDPR, data controllers must consult with the supervisory authority prior to processing if a data protection impact assessment (DPIA) indicates that the processing would result in high risks unless the controller takes measures to mitigate those risks. The DPIA, a requirement under Article 35 of the GDPR for certain types of processing, helps to identify and assess the impact of processing activities on the protection of personal data. If the assessment shows that the processing would still pose a high risk to the rights and freedoms of individuals despite the planned risk mitigation measures, the controller is required to seek the advice of the supervisory authority.

The GDPR, specifically Article 39(1)(e), also outlines the

advisory role of the Data Protection Officer (DPO). The DPO may consult the DPA on any matter relating to the processing of personal data. This provision allows for a broader scope of consultation, not limited to high-risk processing activities, but encompassing any concerns or clarifications that the DPO or the organisation may have regarding data processing practices.

In addition to the GDPR, national laws in EU member states may introduce specific provisions regarding consultation with data protection authorities. For example, Italy's Privacy Code requires consultation with the Italian data protection authority (Garante per la protezione dei dati personali, GPDP) in relation to certain processing activities:

- Medical and scientific research: The specific provisions of articles 110 and 110-bis of the Privacy Code require the consultation or authorisation of the GPDP for the processing of personal data in the context of medical research programmes or other scientific research or statistical purposes, under the conditions set out in these articles.
- Notification requirements for processing in the public interest: Article 2-ter of the Privacy Code, as amended by Legislative Decree No. 139/2022, introduces a notification requirement. It provides that the conditions under which the dissemination and communication to third parties of personal data processed for reasons of public interest or in connection with the exercise of public powers must be notified to the GPDP.

Consultation with data protection authorities is a critical step for data controllers in situations where data processing activities pose significant privacy risks, involve sensitive areas such as health research, or fall under specific regulatory conditions. These consultations serve as a preventive measure to ensure compliance with data protection laws, protect the rights of individuals, and potentially mitigate legal and reputational risks for organisations.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

The General Data Protection Regulation (GDPR) requires a rigorous and proactive approach to mitigating the risks to individuals' rights and freedoms posed by data processing activities. This requirement is deeply embedded in the GDPR and requires data controllers not only to carry out a general analysis of the risks associated with their processing activities, but also, under certain conditions, to carry out a more detailed assessment through the Data Protection Impact Assessment (DPIA) mechanism.

The obligation to conduct a general risk analysis derives from the principle of accountability enshrined in the GDPR, which requires data controllers to take technical and organisational measures that are proportionate to the risks identified. This principle emphasises the need to integrate data protection considerations into processing activities from the outset, thereby ensuring that the principles of data minimisation and security are respected throughout the data processing lifecycle.

In addition, Article 35 of the GDPR sets out the conditions under which a DPIA is required, in particular for processing activities that are considered to pose a high risk to the privacy and rights of natural persons. The Italian data protection authority (Garante per la protezione dei dati personali, GPDP) has further clarified this requirement by publishing a non-exhaustive list of processing operations that require a DPIA. These operations include large-scale processes involving evaluation or scoring functions, automated decision-making processes and the systematic monitoring of sensitive categories of data, including biometric and genetic data.

In the absence of a specific methodology for conducting DPIAs prescribed by the GPDP, the Authority encourages compliance with the "Guidelines on Data Protection Impact Assessment" issued by the Article 29 Working Party (now replaced by the European Data Protection Board). These guidelines, which have been revised, most recently on 4 October 2017, provide a structured approach to conducting DPIAs, emphasising the assessment of processing activities against the background of potential risks to the rights and freedoms of individuals.

The methodology for conducting risk assessments recommended by these guidelines includes the use of established international standards such as ISO 27005, which focuses on information security risk management, and ISO 31000, which provides principles and guidelines for risk management in general. Conducting a DPIA thus involves a meticulous process of identifying the types of personal data processed, assessing the potential risks to the rights and freedoms of data subjects, and implementing the necessary measures to mitigate such risks.

Conducting risk assessments is a comprehensive

undertaking that involves a variety of technical, organisational and administrative procedures. This multifaceted approach may include conducting vulnerability assessments and penetration tests to identify and remediate security vulnerabilities, building threat models to anticipate potential threats and their likely sources, and implementing strict access controls to protect against unauthorised access to personal data.

In essence, the GDPR imposes a mandate on data controllers to adopt a preventative and comprehensive approach to risk assessment in relation to data processing activities. This includes both a general analysis of processing risks, as well as a more detailed assessment through DPIAs in cases where processing activities are likely to result in a high risk to individuals' rights and freedoms. By following the guidance provided by the European Union and incorporating principles from international standards, organisations will be better equipped to navigate the intricacies of risk assessment and thereby ensure that their processing activities are conducted in a manner that is both responsible and consistent with the GDPR's protective objectives.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The General Data Protection Regulation (GDPR), as well as national legislation, outlines specific requirements for organisational roles dedicated to overseeing the critical areas in the complex legal landscape of data protection and cybersecurity. The GDPR, through Article 37.1, mandates the appointment of a Data Protection Officer (DPO) for entities that perform certain types of data processing activities, including public authorities and organisations engaged in large-scale monitoring or processing of sensitive personal data. The Italian Privacy Code, in particular Article 2-sexiesdecies, extends this requirement to judicial authorities that process personal data in their official capacity. The DPO is charged with ensuring compliance with data protection laws, advising data processors and data controllers, acting as a liaison with supervisory authorities and acting as a point of contact for data subjects wishing to exercise their rights.

At the same time, the appointment of a Chief Information Security Officer (CISO), which was already required by Italian law prior to the recent bill, has been recognised as a key role for organisations seeking to strengthen their information security posture. A CISO's responsibilities typically include developing information security strategies, managing risks to information assets, ensuring regulatory compliance and overseeing the implementation of security measures. In particular, DPCM No. 81/2021 emphasises the importance of appointing a designated point of contact for entities within the National Cyber Security Perimeter, who is tasked with overseeing compliance with prescribed organisational and technological security measures.

The bill on strengthening national cyber security marks a significant development in this regulatory environment, proposing the creation of a dedicated internal structure for cyber security activities within entities. This initiative aims to consolidate cybersecurity efforts, supported by the necessary human, instrumental and financial resources, into a coherent and integrated approach to cybersecurity management. A key feature of this law structure is the introduction of a CISO, who will act as the primary point of contact with the National Cybersecurity Agency (ACN). This position is intended to facilitate streamlined communication and collaboration with the ACN, ensuring that entities are kept abreast of relevant cybersecurity information, alerts and updates.

This legislative development reflects a comprehensive approach to improving data protection and cybersecurity governance within organisations. By requiring the appointment of DPOs and proposing the establishment of dedicated cybersecurity structures and contacts, Italian law aims to ensure that organisations not only comply with existing data protection regulations, but also proactively address the challenges posed by the evolving cybersecurity threat landscape. Through these measures, organisations are encouraged to adopt a holistic approach to privacy, data protection and information security, ensuring resilience against breaches and unauthorised access, while upholding the rights of data subjects.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

The importance of employee training is implicitly recognised, if not always explicitly mandated, by various regulations within the data protection and cybersecurity legal framework. The General Data Protection Regulation (GDPR) serves as a fundamental pillar in this regard, emphasising the need for organisations to implement comprehensive organisational security measures. This expectation indirectly calls for the implementation of employee training programs as a critical component of an organisation's privacy and security measures.

Articles 5.2, 29 and 32.4 of the GDPR highlight the principle of accountability and the obligations of data controllers and processors to ensure the security of the processing of personal data. While the GDPR does not specify employee training as a separate requirement, it is understood as an integral organisational security measure. As such, organisations are encouraged to establish ongoing training programs for employees who are authorised to process personal data. Such programmes should ideally begin at the time of initial employment and continue on a regular basis – recommended annually – to reinforce and update employees' knowledge of data protection principles and practices. In addition, maintaining documentation of training attendance and completion is recommended to demonstrate compliance with the GDPR's principle of accountability.

The cybersecurity regulatory landscape, including the PSNC, the Digital Operational Resilience Act (DORA), and the Network and Information Systems Security Directive (NIS2), further underscores the importance of training. These frameworks, while not explicitly mandating training, recognise the critical role of awareness and education in strengthening cybersecurity and personal data protection safeguards.

Collectively, these regulations advocate for the inclusion of cybersecurity and data protection topics in organisational training programmes. By fostering a culture of security awareness, organisations can better equip their employees to recognise, respond to and mitigate cyber threats, contributing to the overall resilience of the organisation against cyber attacks and data breaches. Training is seen as a proactive measure to enhance organisational security, ensure compliance with data protection laws and protect against cyber threats. Organisations are therefore advised to integrate comprehensive training programmes covering key aspects of data protection and cybersecurity into their operating models, and to document these training efforts as part of their compliance and risk management strategies.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Under the General Data Protection Regulation (GDPR), organisations are required to comply with the principle of transparency in the processing of personal data. This principle requires data controllers to provide data subjects with clear, concise and comprehensive information about the processing activities relating to their personal data.

GDPR sets out specific circumstances in which data subjects must be informed about the processing of their personal data:

Article 13 of the GDPR requires that when personal data is collected directly from data subjects, they must be provided with a privacy notice at the time of collection. This notice should detail the purposes of the processing, the legal basis for the processing, the recipients of the data and other relevant information to ensure fair and transparent processing.

Article 14 of the GDPR outlines the requirements for providing information when personal data has not been obtained directly from the data subject. In these cases, the data controller must provide a privacy notice within a reasonable time after obtaining the data, and at the latest within one month, or at the time of the first communication with the data subject, or before the data is disclosed to another recipient.

The GDPR requires information notices to be:

- Written in a manner that is concise, transparent and understandable.
- Easily accessible, using clear and plain language.
- Compliant with the overarching requirements of Article 12 of the GDPR, which emphasises the need to facilitate the exercise of data subjects' rights by providing information in a user-friendly manner.

In order to improve the clarity and accessibility of privacy notifications, the Italian Data Protection Agency (Garante per la protezione dei dati personali, GPDP) launched an initiative aimed to explore the potential of icons, symbols or other graphic elements to simplify privacy notices and make them more understandable to the general public. Following this initiative, the GPDP presented on its website three sets of icons that were found to be the most effective in conveying privacy information in a concise and clear manner.

At its core, the GDPR's strict requirements for privacy notices reflect the regulation's commitment to ensuring that data subjects are fully informed about the processing of their personal data. By mandating the provision of information at the point of data collection or shortly thereafter, and advocating the use of clear, accessible language and innovative visual aids, the GDPR aims to empower individuals with knowledge and control over their personal data. These provisions

underscore the importance of transparency in the digital age, and strengthen the rights of individuals in the face of increasingly complex data processing activities.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The General Data Protection Regulation (GDPR) makes a clear distinction between data controllers and data processors, entities that play different roles in the processing of personal data. This distinction is crucial, as it outlines the responsibilities and obligations that each party has in relation to data protection and GDPR compliance.

Data controllers are the entities (whether individuals, organisations or public authorities) that determine the purposes and means of processing personal data. They have the primary administrative responsibility under the GDPR, and are tasked with ensuring overall compliance with the regulation. This encompasses a wide range of obligations, including but not limited to ensuring that the processing of personal data is lawful, fair and transparent (Article 5 GDPR), responding to data subject rights requests (Articles 15-22 GDPR) and conducting data protection impact assessments where required (Article 35 GDPR). In addition, data controllers are required to establish a legal basis for their processing activities (Article 6 GDPR) and, where applicable, to ensure the protection of data in cross-border transfers.

On the other hand, Data Processors are entities that process personal data on behalf of the data controller. While not directly responsible for determining the purposes and means of processing, processors play a crucial role in handling personal data in accordance with the controller's instructions. Their responsibilities are primarily operational and technical, focusing on implementing the technical and organisational measures necessary to ensure data security (Article 32 GDPR) and keeping records of processing activities under certain conditions (Article 30(2) GDPR).

The GDPR establishes a legal framework that requires data controllers to engage only those data processors that can provide 'sufficient guarantees' to meet the technical and organisational requirements of the GDPR, thereby ensuring the protection of data subjects' rights (Article 28 GDPR). This implies an obligation of due diligence on the part of data controllers when selecting their processors. In addition, the relationship between controllers and processors must be governed by a contract or other legal act setting out the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller (Article 28(3) GDPR).

While many of the GDPR's obligations are imposed directly on data controllers, data processors are not exempt from compliance. By operation of law, data processors are subject to specific obligations under the GDPR. This regulatory approach is further cemented by contractual agreements between controllers and processors, which extend the GDPR's obligations to processors and ensure a cohesive data protection strategy.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Specific obligations are imposed directly on data processors by operation of law. In addition, the GDPR requires certain minimum contractual terms to be established between data controllers and data processors to ensure the protection of personal data.

Data processors are not simply third-party service providers, but are entrusted with significant legal obligations under the GDPR. These include, but are not limited to

- Processing personal data only on the basis of documented instructions from the controller (Article 28(3)(a) GDPR).
- Ensuring that persons authorised to process personal data are bound by confidentiality obligations (Article 28(3)(b) GDPR).
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Article 32 GDPR).
- Assisting the controller in ensuring compliance with the obligations under Articles 32 to 36 on security of processing, notification of personal data breaches and data protection impact assessments (Article 28(3)(f) GDPR).

These obligations ensure that processors contribute significantly to the overall protection of personal data within the processing ecosystem.

According to Article 28(3) GDPR, the engagement of a processor by a controller must be governed by a

contract or other legal act in accordance with Union or Member State law. This contract must specify

- The scope and duration of the processing.
- The nature and the purposes of the processing.
- The nature of the personal data and the categories of data subjects.
- The controller's obligations and rights.

It must also explicitly specify the processing instructions, including the transfer of personal data to third countries or international organisations, and impose specific obligations on the processor to ensure data protection. The contract acts as a binding document that aligns the processor's activities with the requirements of the GDPR, ensuring accountability and transparency in the processing of personal data.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

Beyond setting minimum contract terms, the GDPR imposes several other restrictions and requirements on controllers when appointing processors to handle personal data, emphasising the importance of due diligence, privacy and security assessments.

- Due Diligence

Data controllers are required to conduct thorough due diligence before appointing a data processor. This involves assessing the processor's capabilities and practices in handling personal data, and ensuring that they can provide sufficient guarantees to meet the GDPR's technical and organisational measures. The due diligence process helps controllers ensure that processors are compliant with GDPR standards, and can effectively uphold data protection principles.

- Privacy and security assessments

Privacy and security assessments are critical elements of the processor selection process. Controllers must assess the processor's privacy policy, security infrastructure and compliance track record. This includes reviewing the processor's data breach prevention, data minimisation and data subject rights protection measures. Controllers are also expected to periodically review and monitor the processor's compliance with the GDPR, which may include conducting audits or requiring the processor to undergo certifications or third-party audits that demonstrate compliance with data protection standards.

- Other restrictions

The GDPR requires that processors should not engage another processor (sub-processor) without prior specific or general written authorisation from the controller (Articles 28(2) and 28(4) GDPR). This ensures the controller's oversight of the entire processing chain. Furthermore, where a processor engages a sub-processor, the same data protection obligations as set out in the contract between the controller and the processor must be imposed on the sub-processor, ensuring a consistent level of protection of personal data throughout the processing chain.

The GDPR establishes a comprehensive framework for the obligations and responsibilities of data processors, including specific requirements for contracts between controllers and processors, due diligence and ongoing assessments. These provisions ensure that personal data is processed securely and in compliance with the law, reflecting the GDPR's commitment to data protection and privacy.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

In Italy, the robust framework of the General Data Protection Regulation (GDPR) of the European Union (EU) governs the realms of data protection and privacy, delineating clear definitions and stringent restrictions on practices such as monitoring, automated decision-making, and profiling, which significantly impact individual privacy rights.

Monitoring, within the GDPR context, is understood as the comprehensive observation and tracking of an individual's activities across diverse digital landscapes. This includes scrutinizing location data, IP addresses, and various online identifiers to map a person's behavior over time and across multiple platforms. Similarly, automated decision-making is characterized by decisions made entirely through automated processes, devoid of human oversight, which bear significant consequences for individuals. Profiling emerges as a nuanced form of automated processing, aimed at assessing personal attributes, such as work performance, economic status, health conditions, and personal preferences, to predict or analyze pertinent aspects of an individual's life.

The GDPR mandates unequivocal transparency and

informed consent for activities involving monitoring, automated decision-making, and profiling. Organizations are compelled to disclose the nature of data collection, its intended use, and the potential outcomes to individuals, ensuring an option for consent withdrawal at any given time.

Specifically, the regulation casts a critical eye on profiling and automated decisions that have legal or substantial impacts on individuals, such as loan denial, typically barring such practices unless underpinned by legal authorization, contractual necessity, or explicit consent from the individual concerned. Moreover, profiling that leverages special categories of data, touching upon sensitive aspects like racial or ethnic origin, political opinions, or religious beliefs, faces strict prohibitions, save for a few narrowly defined exceptions.

In the sphere of tracking technologies, such as cookies, Italian regulations demand that websites and applications secure explicit, informed consent from users before deploying these tools on user devices. This involves the implementation of transparent, easily navigable cookie consent mechanisms that articulate the purpose behind the use of cookies, thereby empowering users to make informed choices about their consent.

The Garante per la protezione dei dati personali, Italy's Data Protection Authority, plays a pivotal role in upholding the GDPR, equipped with the authority to conduct investigations, levy fines for non-compliance, and mandate the cessation of processing activities found in violation of the regulation.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

The conceptual framework surrounding the practices of targeted advertising and cross-contextual behavioral advertising remains unencapsulated within the explicit letter of the General Data Protection Regulation (GDPR). Nevertheless, the regulation's foundational principles concerning data processing and the sacrosanct rights of individuals become particularly pertinent in the oversight of such practices within the jurisdiction of Italy.

In the realm of Targeted Advertising, it becomes evident that the GDPR's ambit is invoked when the advertising methodologies entail the processing of personal data, such as browsing proclivities or demographic information, for the purpose of advertising. It is incumbent upon organizations to establish a lawful predicate for such data processing, with consent being a paramount consideration. Furthermore, the principle of transparency assumes critical importance, necessitating that individuals be duly apprised of the nature of data collection, its utilization for targeting purposes, and the provision of an avenue for opting out.

The practice of Cross-Contextual Behavioral Advertising (CCBA), which amalgamates user data across disparate websites or applications to construct targeted advertising profiles, engenders additional considerations under the GDPR. The transfer of personal data across varying contexts for advertising ends likely necessitates the explicit consent of the concerned individual. Entities engaging in CCBA must manifest adherence to the GDPR tenets of data minimization, purpose limitation, and data security.

While the GDPR does not proffer specific delineations for targeted advertising or CCBA, it articulates related concepts such as:

– Profiling, which involves the analysis of personal data to anticipate aspects of an individual's behavior or predilections, serving as a cornerstone of targeted advertising.

– The Processing of Personal Data, a broad term that encapsulates any operation performed upon personal data, including its collection, storage, utilization, and transmission, with targeted advertising and CCBA falling within its purview.

The GDPR, while not outrightly proscribing targeted advertising or CCBA, imposes restrictions through its core principles, necessitating a lawful basis for personal data processing, ensuring transparency and upholding individual rights, advocating for data minimization, enforcing purpose limitation, and mandating data security.

The Italian Data Protection Authority stands vested with the powers to conduct inquiries and enforce GDPR compliance in relation to targeted advertising and CCBA, potentially levying fines or mandating alterations in organizational practices for non-compliance.

In sum, while neither targeted advertising nor CCBA are explicitly interdicted under the GDPR, the regulation imposes stringent constraints to safeguard user privacy and data autonomy. Organizations within Italy must ensure their operations are in strict conformity with these regulatory stipulations to avert potential enforcement actions.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

The General Data Protection Regulation (GDPR), which is applicable within the Italian jurisdiction, governs the transactional aspects of personal data, albeit without furnishing an explicit definition of the term "sale" in this context. The regulation delineates several foundational concepts and imposes a framework of restrictions on the dissemination of personal data, ostensibly regulating its sale through indirect mechanisms, there not explicit reference to sales in Italy.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Organizations in Italy conducting electronic direct marketing campaigns must ensure they have a lawful basis for processing personal data, typically through freely given consent. Transparency and clear opt-out mechanisms are crucial. Specific national rules might apply to phone calls depending on whether the target is a consumer or business. Non-compliance with these regulations can lead to enforcement actions by the Italian Data Protection Authority.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

The recent Provision of February 22th, 2024 of the Data Protection Authority outlines the restrictions imposed. Based on the provision provided, it becomes apparent that the jurisdiction under discussion adheres to stringent regulations concerning the processing of biometric data, such as facial recognition, particularly within the context of employment. The legal framework governing these practices is rooted in the General Data Protection Regulation (GDPR), as evidenced by the references to various articles within the provision. The focal point of the discussion revolves around a specific instance where an authority, presumably a Data Protection Authority, has deemed the processing of biometric data for attendance monitoring purposes as unlawful.

The regulation defines biometric data (referenced under Article 9 of the GDPR) as personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that person, such as facial images. The use of biometric data, therefore, is subject to rigorous scrutiny and requires adherence to the foundational principles of the GDPR, including legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.

The provision outlines that the processing of employees' biometric data (specifically facial recognition) by a company, for the purpose of attendance tracking, contravened several GDPR principles and articles, including but not limited to:

– Article 5(1)(a) which mandates that personal data must be processed lawfully, fairly, and in a transparent manner.

– Article 9 that stipulates special conditions for processing sensitive data categories, which include biometric data.

– Articles 13, 28, 30, 32, and 35, which encompass requirements for data processing transparency, processor relationships, records of processing activities, security of processing, and data protection impact assessments, respectively.

The authority concluded that the violations were not minor, considering the nature of the breach that violated general principles and conditions for lawful data processing. The seriousness of the violation, the degree of responsibility, and the manner in which the violation was discovered were also taken into account.

In response to the investigation, the company reportedly suspended biometric data processing operations and outlined a procedure for decommissioning the biometric devices, including the deletion of data stored on devices at the end of the procedure initiated by the supervisory authority.

As a corrective measure, the authority imposed a monetary administrative fine, as provided under Article 83 of the GDPR, which is determined based on the specifics of the case and in accordance with Article 58(2)(i) of the GDPR.

In essence, this provision illustrates the application of

the GDPR's stringent requirements on the processing of biometric data, emphasizing the need for lawful basis, transparency, and robust security measures to protect such sensitive data. Organizations operating within this jurisdiction must ensure compliance with these regulations to avoid enforcement actions, including substantial fines.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

In Italy, the domain of artificial intelligence (AI) is navigated without the aid of specific laws or regulations dedicated solely to this advanced technology. The Italian stance towards the governance of AI is integrated within the broader, well-established framework of the General Data Protection Regulation (GDPR), thereby addressing the conceivable risks associated with the processing of data through AI by leveraging existing legal norms.

This integration sees the GDPR's provisions being applied to the realm of AI with particular emphasis on ensuring that there is transparency and explainability in automated decision-making processes. This necessity arises especially when such decisions have the potential to significantly affect individuals, legally or otherwise. In such instances, organizations employing AI for decision-making are tasked with the responsibility of making the logic behind their algorithms and the data employed in training these systems comprehensible and accessible to those affected.

Moreover, the principles of data minimization and purpose limitation, cornerstone concepts of the GDPR, are also of paramount importance in the context of AI. These principles mandate that organizations collect and utilize only the data that is strictly necessary for the intended AI application and are clear about the purposes for which this data is processed. The regulation identifies certain uses of AI, such as facial recognition and profiling for evaluating work performance, as high-risk. Such applications are subjected to more stringent risk assessments and might necessitate additional safeguards to mitigate concerns related to data protection.

Recent activities by the Italian Data Protection Authority highlight its vigilance and proactive stance in scrutinizing AI practices. For instance, in 2023, the authority conducted investigations into how companies gather data for the purpose of training AI systems. These investigations underscored the critical importance of obtaining user consent and adhering to proper data handling practices.

Looking forward, the regulatory landscape for AI in Italy is poised for evolution, influenced by comprehensive AI regulations being formulated at the European Union level. This development signifies a potential shift towards more specialized legislation in the future.

Despite the current absence of AI-specific laws, the framework provided by the GDPR lays a robust foundation for the responsible development and deployment of AI technologies. This approach ensures the protection of individual data privacy rights, necessitating organizations to remain abreast of legislative developments within the EU and to align their AI practices with the GDPR's stringent principles and any forthcoming regulations.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

According to the national and European Union legal framework, particularly the General Data Protection Regulation (GDPR), the transfer of personal data to countries outside the European Economic Area (EEA) is subject to strict conditions. Such transfers are only permitted if the European Commission has determined that the recipient country provides an adequacy level of data protection, as set out in Article 45 of the GDPR. In the absence of such an adequacy decision, personal data may still be transferred outside the EEA provided that the *data exporter* – whether a data controller or a data processor – implements appropriate protective measures as set out in Article 46(2) and (3) of the GDPR, including, but not limited to, the use of standard contractual clauses.

If the above conditions are not fulfilled, the GDPR allows the transfer of personal data to a third country under specific derogations for exceptional situations, as described in Article 49. Such derogations include, for example, the explicit consent of the data subject to the proposed transfer.

In this legal context, the Court of Justice of the European Union (CJEU), in its judgment of 16 July 2020 in Case C-311/18 (known as the "Schrems II" case), invalidated the EU-US Privacy Shield framework, but confirmed the legitimacy of standard contractual clauses as a

mechanism for data transfer, subject to the data exporter's assessment of whether the law or practice in the third country affects the effectiveness of the protective measures set out in Article 46 of the GDPR. The CJEU also underlined that data transfers to third countries must not undermine the level of protection guaranteed within the EEA.

Following this ruling, the European Data Protection Board (EDPB) issued two sets of guidelines to help ensure compliance with the data transfer rules: "*Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" adopted on 18 June 2021 after public consultation and "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*" of 10 November 2020.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

In the legal landscape shaped by the European Union's General Data Protection Regulation (GDPR), a sophisticated and layered approach to data protection is mandated, highlighting the critical role of both data controllers and processors in ensuring the integrity and confidentiality of personal data. The cornerstone of this approach is Article 32 of the GDPR, which outlines the requirement for the implementation of technical and organisational measures that are precisely calibrated to the level of risk associated with different data processing activities. This calibration requires taking into account both the 'context' of the processing – the specific conditions and characteristics unique to each processing scenario – and the 'state of the art', referring to the latest advances in data protection technologies and methodologies.

The Italian legal framework, in particular through the provisions of DPCM 81/2021 and its Annex B, echoes and builds on these GDPR principles by specifying a series of detailed and structured security measures. These measures are not simply presented as a checklist, but are categorised to reflect the multifaceted nature of data security, which includes:

- Strategic organisational measures, which include policies, procedures and privacy impact assessments to ensure that privacy is woven into the fabric of organisational practices.
- Physical security measures, which address the security of the physical environment in which personal data is stored and processed, from access controls to the secure disposal of the assets that hold the data.
- Logical and technological measures to protect data from cyber threats, including encryption, secure access controls and regular security assessments.
- Protocols for the secure management, storage and transmission of data to ensure that data is protected both at rest and in transit.

This comprehensive framework, set out in Annex B, is based on the principles of adaptability and technological development. It requires organisations not only to assess the risks specific to their data processing activities, but also to keep up-to-date with the latest security technologies and best practices and incorporate them into their data protection strategies. This dynamic and proactive approach to data security is critical in a landscape where cyber threats are constantly evolving and becoming more sophisticated.

The European Union Agency for Cyber security (ENISA) supports these efforts through its publications, including the 'Handbook on Security of Personal Data Processing' and the 'Technical Guidelines for the implementation of minimum security measures for digital service providers'. These documents provide a wealth of knowledge and guidance, outlining the minimum technical standards and security measures that should be in place for personal data processing and digital services respectively. They offer an invaluable resource for organisations seeking to navigate the complex area of GDPR compliance, providing insight into best practice, technical standards and the implementation of effective security measures.

By integrating GDPR principles with national regulations and ENISA's expert guidance, organisations are equipped with a robust data protection framework. This framework not only mandates the protection of personal data from unauthorised access and threats, but also promotes a culture of continuous improvement and adaptation to technological advances. As a result, the legal and regulatory landscape in the EU and its Member States represents a comprehensive and forward-looking approach to data security, ensuring that the rights and freedoms of data subjects are protected in an increasingly digital world.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

In the jurisdiction of the European Union and its Member States, including Italy, the legal framework for data protection, privacy and cybersecurity has evolved to address the complexities of security breaches with a multi-faceted approach, primarily underpinned by the General Data Protection Regulation (GDPR) and complemented by recent legislative developments such as the NIS2 Directive.

Under GDPR, a "personal data breach" has been meticulously defined in Art 4(12) as a breach of security that leads to personal data being destroyed, lost, altered, disclosed or accessed without authorization in transmission, storage or other processing. This definition encompasses different forms of compromise that may affect the integrity, availability and confidentiality of personal data, and categorises breaches into:

- Breaches of confidentiality, where personal data is disclosed or accessed by unauthorised parties;
- Breaches of integrity, which involve the unauthorised or accidental modification of personal data;
- Breaches of availability, where data is lost or access to it is impeded or unlawfully destroyed.

The Article 29 Data Protection Working Party, in its 2014 opinion, and ENISA, through its 2020 threat landscape publication, have contributed to the understanding and classification of personal data breaches, highlighting the role of human error and the potential for malicious intent behind these incidents.

Beyond GDPR, the NIS2 Directive (which replaces the original NIS Directive) extends the scope of cybersecurity obligations to a wider range of sectors and introduces more stringent security and incident reporting requirements. While NIS2 does not explicitly redefine "security breach", it emphasises the need for significant network and information system security and requires enhanced measures against cybersecurity threats and incidents that could disrupt the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data.

In the Italian context, Legislative Decree No. 65/2018 further defines an "incident" in the field of network and information systems security as any event having an actual adverse effect, in line with the broader European regulatory perspective.

The National Cybersecurity Perimeter (Perimetro di Sicurezza Nazionale Cibernetica – PSNC) framework, while not explicitly defining a "security incident", is instrumental in strengthening the cybersecurity posture of Italy's critical infrastructure and digital ecosystem. In this framework, a security incident is defined as any event or sequence of events that compromises the confidentiality, integrity or availability of information systems, networks or data.

These legal instruments together provide a comprehensive legal framework for addressing security breaches, with precise definitions and categorisations of breaches and incidents. They work together to enforce a robust approach to cybersecurity that emphasises prevention, preparedness, response and recovery across different sectors, ensuring the resilience of the digital and financial ecosystem against a backdrop of escalating cyber threats.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

In Italy, the domain of artificial intelligence (AI) is navigated without the aid of specific laws or regulations dedicated solely to this advanced technology. The Italian stance towards the governance of AI is integrated within the broader, well-established framework of the General Data Protection Regulation (GDPR), thereby addressing the conceivable risks associated with the processing of data through AI by leveraging existing legal norms.

This integration sees the GDPR's provisions being applied to the realm of AI with particular emphasis on ensuring that there is transparency and explainability in automated decision-making processes. This necessity arises especially when such decisions have the potential to significantly affect individuals, legally or otherwise. In such instances, organizations employing AI for decision-making are tasked with the responsibility of making the logic behind their algorithms and the data employed in training these systems comprehensible and accessible to those affected.

Moreover, the principles of data minimization and purpose limitation, cornerstone concepts of the GDPR, are also of paramount importance in the context of AI. These principles mandate that organizations collect and utilize only the data that is strictly necessary for the intended AI application and are clear about the purposes for which this data is processed. The regulation identifies certain uses of AI, such as facial recognition and profiling for evaluating work performance, as high-risk. Such applications are subjected to more stringent risk assessments and might necessitate additional safeguards to mitigate concerns related to data protection.

Recent activities by the Italian Data Protection Authority highlight its vigilance and proactive stance in scrutinizing AI practices. For instance, in 2023, the authority conducted investigations into how companies gather data for the purpose of training AI systems. These investigations underscored the critical importance of obtaining user consent and adhering to proper data handling practices.

Looking forward, the regulatory landscape for AI in Italy is poised for evolution, influenced by comprehensive AI regulations being formulated at the European Union level. This development signifies a potential shift towards more specialized legislation in the future.

Despite the current absence of AI-specific laws, the framework provided by the GDPR lays a robust foundation for the responsible development and deployment of AI technologies. This approach ensures the protection of individual data privacy rights, necessitating organizations to remain abreast of legislative developments within the EU and to align their AI practices with the GDPR's stringent principles and any forthcoming regulations.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

In Italy, the landscape for data breach notification is not solely defined by the General Data Protection Regulation (GDPR) of the European Union (EU); it is further nuanced by an array of regulations that cater to specific sectors or entities. These regulatory frameworks are designed to ensure that entities are well-prepared to manage and report security incidents, thus safeguarding the integrity and resilience of critical infrastructure and sensitive data.

The NIS Directive, formally recognized as Directive (EU) 2016/1148, establishes foundational security and incident notification guidelines for operators of essential services. It mandates that significant security incidents, with the potential to disrupt the provision of vital services, be reported to national Computer Security Incident Response Teams (CSIRTs).

Building upon the foundational measures set forth by the NIS Directive, the NIS2 Directive, or Directive (EU) 2022/2475, ushers in a regime of enhanced obligations concerning incident response and notification for entities deemed "essential" or "important" within critical sectors. This directive not only emphasizes the necessity for implementing technical and organizational measures to counter cybersecurity risks but also mandates the appointment of dedicated personnel or teams for incident management.

The Digital Operational Resilience Act (DORA) addresses the financial sector, prescribing stringent incident response and notification protocols to counteract IT and operational vulnerabilities. Financial institutions are obliged to communicate any substantial incidents to the European Central Bank (ECB), highlighting the potential repercussions on their operational capabilities or the broader financial system.

Furthermore, Italy is in the process of developing the "Perimetro di sicurezza nazionale cibernetica" (National Cybersecurity Perimeter), which aims to delineate and secure critical national infrastructures against cyber threats. Anticipated to include incident response and notification mandates, this regulation will play a pivotal role in strengthening national cybersecurity defenses.

Summarily, alongside the GDPR's mandate for organizations to alert the Garante and affected individuals of breaches posing a significant risk to personal rights and freedoms, Italy's regulatory framework is extensive. It encompasses the NIS Directive's emphasis on critical infrastructure, the NIS2 Directive's augmented requirements for critical sector entities, DORA's focus on the financial industry's resilience, and the prospective national cybersecurity perimeter's broad protective scope.

Entities operating within Italy are advised to cultivate comprehensive incident identification, assessment, and reporting protocols, aligning with legal obligations and best practice recommendations. Vigilance and adaptability to the evolving regulatory environment in Italy and across the EU are essential to ensure ongoing compliance with the diverse spectrum of data breach notification requirements.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Italy, amidst the global concern over cybercrime, particularly ransom payments in ransomware attacks,

demonstrates a robust legal framework albeit without singular legislation specifically targeting ransom payments. The nation's approach to cybercrime, underpinned by its criminal code, encompasses a range of illicit activities including unauthorized access to computer systems, data manipulation, and cyber extortion. Although specific guidance on handling ransomware payments remains somewhat limited, such payments could fall under scrutiny in cyber extortion investigations pursuant to the nation's existing legal apparatus.

The stance of Italian authorities leans towards a proactive incident response, advocating for immediate reporting of cybercrime incidents and fostering collaboration with law enforcement to enhance the prospects of identifying offenders and recovering compromised data.

Globally, the narrative around ransomware is intensifying, with numerous countries like the United States, United Kingdom, and Australia, among others, refining their legislative and policy frameworks to specifically address this menace. Common strands across these national approaches include the imposition of reporting mandates for ransomware incidents, a general discouragement of ransom payments to deter the perpetuation of cybercriminal activities, and the promotion of information sharing to forge a collective defense against cyber threats.

For organizations ensnared by ransomware within Italy and elsewhere, navigating the intricate legal and financial implications of potential ransom payments is paramount, necessitating expert legal counsel. Moreover, engagement with law enforcement not only fulfills a civic duty but also opens avenues for investigation and recovery operations.

In summation, while Italy may not feature standalone legislation regarding ransomware payments, its legal provisions coupled with an emphasis on incident reporting and cooperation with law enforcement agencies, reflect a comprehensive strategy towards cybercrime. This resonates with the broader international momentum towards fortifying defenses against ransomware, underscoring the imperative of legal compliance and collaborative efforts in combating cyber threats.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The National Cybersecurity Agency (Agenzia per la cybersicurezza nazionale, ACN) stands as a pivotal institution within Italy's cybersecurity framework, having been instituted by a decree in June 2021. Operating under the auspices of the Prime Minister's Office, the ACN is endowed with the mission of protecting national interests within the cyberspace domain.

At the heart of its mandate, the ACN is tasked with the resilience and security of the nation's critical infrastructure and information systems against cyber threats. It embodies the central coordinating force for cybersecurity measures across various public sectors and is recognized as the national authority in cybersecurity. This entails setting strategic directions and guidelines for the cybersecurity sector, alongside nurturing the growth of a national cybersecurity industry through the encouragement of innovation and entrepreneurship.

The organizational architecture of the ACN includes integral units such as the Computer Security Incident Response Team (CSIRT), responsible for managing cybersecurity incidents that impact national interests and critical infrastructure. Additionally, the National Assessment and Certification Center (CVCN) undertakes the assessment and certification of security measures for Information and Communication Technologies (ICT) products and services integral to national infrastructure operators. The National Coordination Centre, meanwhile, ensures the coherent orchestration of national cybersecurity endeavors and fosters collaboration with international allies.

In essence, the ACN is instrumental in fortifying Italy's digital infrastructure against evolving cyber threats. By serving as the nexus for national cybersecurity initiatives, the agency catalyzes cooperation and innovation, significantly contributing to the enhancement of Italy's cybersecurity posture and cyber resilience.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

The General Data Protection Regulation (GDPR) enshrines a series of personal data protection rights that empower individuals within its jurisdiction, giving them greater control over their personal data. These rights, detailed in Articles 15-22 of the GDPR, include the right to access personal data, to rectify inaccuracies, to erase

data under the 'right to be forgotten', to restrict processing, to transfer data to another controller, to object to processing, and to avoid being subjected to automated decision making and profiling. These provisions are designed to facilitate a transparent interaction between data subjects and data controllers, allowing individuals to effectively manage their personal data.

To exercise these rights, individuals can make requests directly to the data controller managing their personal data. The GDPR requires data controllers to respond promptly, usually within one month, with provisions to extend this period depending on the complexity of the request. Despite these broad rights, the GDPR and the Italian Privacy Code (through Articles 2-undecies and 2-duodecies) recognise certain exceptions and limitations. These are designed to balance the individual's right to privacy with other important interests, such as public security or public health. For example, the right to erasure may not apply where processing is necessary for freedom of expression, compliance with legal obligations or the performance of tasks in the public interest.

Overall, the GDPR establishes a robust framework for data protection that provides individuals with significant rights over their personal data, while also taking into account the need for restrictions to safeguard other societal and individual interests. This regulatory approach highlights the importance of privacy and data protection in the digital age, ensuring that individuals have the means to control their personal data within a balanced legal framework.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Under the provisions of the General Data Protection Regulation (GDPR), individuals are provided with robust mechanisms to enforce their data protection rights, allowing them to use both regulatory and judicial remedies. Under Articles 77 et seq. of the GDPR, data subjects have the right to appeal to a supervisory authority if they believe that the processing of their personal data is in breach of the regulation. This pathway provides a regulatory means for individuals to seek redress and ensure compliance with data protection laws.

In addition to regulatory complaints, the GDPR explicitly provides for the right to an effective judicial remedy. This is particularly relevant when individuals feel that their data protection rights have been violated, or when their complaints to supervisory authorities do not yield satisfactory results. The judicial remedy allows data subjects to bring their grievances directly before the courts, providing an additional layer of protection and enforcement of their privacy rights.

The Italian Privacy Code further supports these GDPR provisions by outlining specific circumstances in which privacy rights may be delayed, limited or excluded (Article 2-undecies). In such cases, individuals retain the ability to exercise their rights through the supervisory authority, as detailed in Article 160 of the Privacy Code. This reinforces the dual framework for rights enforcement, providing both regulatory and judicial channels to address and remedy potential violations of data protection rights.

Taken together, these mechanisms underscore a comprehensive approach to the protection of individuals' data privacy rights within the jurisdiction, ensuring that individuals have access to both regulatory and judicial means to enforce their rights under the GDPR.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Individuals who believe their personal data has been processed in violation of the GDPR have the legal entitlement to pursue a private right of action. This includes the ability to lodge a complaint with the supervisory authority, as outlined in Articles 77 of the GDPR, as well as Articles 141-144 and 153 ff. of the Privacy Code, alongside provisions in Law No. 689/81. Individuals have the right to an effective judicial remedy against data controllers, data processors, and legally binding decisions of the supervisory authority that concern them. This right is specified in Articles 78 and 79 of the GDPR, Article 152 of the Privacy Code, and Article 10 of Legislative Decree No.150/2011. Data subjects may exercise these rights independently or through a mandate to organizations representing their interests, pursuant to Article 80 GDPR.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Article 82 of the GDPR confirms the right of data subjects

to receive compensation for both material and non-material damages resulting from unlawful data processing. Similarly, the Italian Civil Code, through Articles 2043 ff., requires that compensation be awarded only when harm to the right to personal data protection is manifested as actual financial or non-financial damage. Italian cybersecurity legislation outlines various offenses, including unauthorized access to computer systems, possession of access devices, data damage, and computer fraud. Sanctions may be imposed by the legal system following the reporting of a crime, and damages may be pursued through civil litigation.

43. How are data protection laws in your jurisdiction enforced?

The enforcement of data protection, privacy and cybersecurity laws is characterised by a comprehensive framework that includes both regulatory oversight and recourse to the courts. The Italian Data Protection Authority (Garante per la protezione dei dati personali, GPDP), an independent administrative authority, plays a central role in supervising compliance with data protection legislation, thereby safeguarding individuals' fundamental rights and freedoms with regard to the processing of personal data.

The DPA has the power to conduct investigations into reported incidents or potential breaches, which may include requesting information, conducting on-site audits or inspections, and interviewing key individuals involved. Following an investigation, the authority will assess whether there has been a breach of relevant laws or regulations. In cases of non-compliance, the GPDP can impose significant administrative fines of up to €20 million or 4% of the global annual turnover of the responsible company, whichever is higher. It also has the power to order the cessation or suspension of data processing activities for serious breaches.

Individuals affected by violations have the right to seek effective judicial remedies. This includes the possibility to have recourse to ordinary judicial authorities to enforce their rights under the GDPR, such as access, rectification, erasure or restriction of the processing of their personal data. In addition, Italy works closely with data protection authorities from other EU member states to ensure consistent cross-border application of the GDPR, which is particularly important for companies operating in multiple member states. Individuals are entitled to due process, including being notified of the allegations against them, the opportunity to respond to those allegations, and the right to appeal against any penalties imposed. This procedural framework ensures that individuals' rights are adequately protected throughout the data protection enforcement process.

Italy's approach to data protection, privacy and cybersecurity enforcement is characterised by a robust regulatory oversight mechanism and judicial remedies, underpinned by significant penalties and international cooperation, to ensure effective protection of individuals' rights in the processing of personal data. This system reflects a balanced and comprehensive strategy to protect personal data in a complex digital landscape.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

In Italy, adherence to data protection norms is governed by the General Data Protection Regulation (GDPR), which sets forth a comprehensive framework for penalizing non-compliance through administrative fines. This approach underscores Italy's commitment to upholding data privacy without resorting to criminal penalties, a stance that distinguishes it from some other European Union member states.

The Italian Data Protection Authority, known as the Garante per la protezione dei dati personali, is vested with the authority to levy substantial administrative fines against entities that contravene GDPR stipulations. These fines are not nominal; they are designed to serve as a significant deterrent, with the ceiling set at either €20 million or up to 4% of an entity's global annual turnover for the previous financial year, depending on which amount is greater. This structure ensures that the fines are not only punitive but also proportionate to the scale of the infringement and the economic stature of the offending entity.

The determination of fine amounts is a nuanced process that takes into account various factors, including the severity and duration of the infringement, the entity's intent or negligence, its level of cooperation with regulatory authorities, and any mitigating circumstances that might alleviate the gravity of the offense.

In a move towards transparency and deterrence, the Garante is empowered to publicize details about imposed fines, including key excerpts or the entirety of the decision. This publication does not anonymize the names of the fined entities, serving both as a specific deterrent to the entities involved and a general deterrent to the broader market.

Illustrative cases, though not uniformly disclosed in full detail, highlight the range of violations that can incur such fines. These include, but are not limited to, inadequate data protection measures and unauthorized

data sharing or processing activities. Such cases serve as cautionary tales for organizations, emphasizing the critical need for robust data protection practices.

The regime of administrative fines in Italy serves as a stark reminder of the critical importance of GDPR compliance for organizations operating within its jurisdiction. The potential for significant financial penalties, coupled with the reputational damage that can arise from public disclosure of non-compliance, compels organizations to prioritize data protection and invest in the necessary safeguards to ensure adherence to the GDPR's stringent requirements.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Indeed, there exists a structured framework and set of guidelines concerning the computation of fines and the criteria for levying sanctions under the General Data Protection Regulation (GDPR). A notable resource in this context is the publication by the European Data Protection Board (EDPB).

The EDPB, an entity that represents a consortium of data protection authorities from each European Union member state, has issued "Guidelines 04/2022 on the calculation of administrative fines under the GDPR." This document serves as a comprehensive guide for supervisory bodies, including the Italian Data Protection Authority, delineating a methodological approach to determining the magnitude of GDPR fines.

This guidance document is instrumental in ensuring a harmonized application of the GDPR across member states, providing a clear and methodical framework for the assessment and imposition of administrative fines. It underscores the commitment to uphold data protection principles and the integrity of personal data management practices, ensuring that supervisory authorities have a solid basis for enforcing compliance and sanctioning violations.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes, controllers operating in the Italian jurisdiction can appeal to the courts against orders of the regulators, including the Italian Data Protection Authority (Garante per la protezione dei dati personali), regarding GDPR violations.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

The trends in compliance and enforcement practices within the data protection realm are primarily shaped by the inspections conducted by the authority. This approach ensures that the authority's oversight activities directly inform the identification of prevailing trends, enabling a dynamic and responsive regulatory environment. Through such inspections, the authority not only assesses adherence to data protection laws but also identifies areas requiring heightened attention or improvement, thereby guiding entities towards best practices and ensuring the protection of personal data.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

Yes. One of the proposals/regulations under consideration to reform the current EU legal framework on the protection and circulation of personal data is the Digital Services Act (DSA). The DSA specifically targets the regulation of online intermediary services based on their role, size and impact on the online ecosystem. The DSA entered into force on 16 November 2022, and its provisions will be applied from 17 February 2024.

In Italy, Agcom has been designated as the Digital Services Coordinator (DSC) under Legislative Decree No. 123 of 2023. An important collaboration has been established between Giacomo Lasorella, President of Agcom, and Roberto Viola, Director General of DG CONNECT at the European Commission. This partnership aims to support the implementation of the DSA regulations by establishing a procedural framework for the exchange of information and methodologies.

The Data Governance Act (DGA), which came into force on 23 June 2022 and applies from 24 September 2023, is a key piece of European Union legislation that aims to create a comprehensive framework to facilitate data sharing. The Act aims to increase trust in the sharing process, improve the availability of data and support the development of a common European data space, thereby fostering the digital economy in the EU. Furthermore, the Data Act, officially known as Regulation (EU) 2023/2854, marks another important step in the European Union's ongoing efforts to refine its digital and data governance framework. Published in the Official Journal of the European Union on 13 December 2023, the regulation is due to come into force on 12 September 2025. The Digital Markets Act (DMA), which came into

force on 1 November 2022, targets large companies that provide core platform services in the EU, such as online marketplaces and search engines, and designates them as ‘gatekeepers’. These rules, which aim to ensure fair competition and prevent anti-competitive practices, apply from 2 May 2023. Gatekeepers must comply with certain obligations within six months of their designation. In line with the DMA, Italy’s recent competition law strengthens the powers of the Italian Competition Authority (AGCM) to regulate the digital market, with an emphasis on fair competition and consumer protection in the digital space. This coordination with the European Commission ensures a consistent regulatory approach across the EU. It’s worth mentioning the European Union’s AI Act, which will have a significant impact on national legislation. This key piece of legislation aims to regulate the use of artificial intelligence across the EU, emphasising the creation of trustworthy AI through a risk-based approach. It categorises AI systems according to their potential risks, with strict measures imposed on those classified as high risk. The law aims to protect fundamental rights, foster innovation, and ensure transparency and accountability. As the legislative process nears completion, it’s important for stakeholders to prepare for its imminent enactment.

Contributors

Paolo Balboni
Founding Partner
paolo.balboni@ictlc.com

Luca Bolognini
Founding Partner
luca.bolognini@ictlc.com

Francesco Capparelli
Chief Cyber Security Advisor
francesco.capparelli@ictlc.com

Isabella Oldani
Senior Associate
isabella.oldani@ictlc.com