Legal 500
Country Comparative Guides 2025

Italy
Data Protection & Cybersecurity

Contributor

ICT Legal Consulting

Luca Bolognini

Founding Partner | luca.bolognini@ictlc.com

Paolo Balboni

Founding Partner | paolo.balboni@ictlc.com

Francesco Capparelli

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

Nicolò Maria Salvi

Partner | nicolo.salvi@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; what sectors, activities or data do they regulate; and who enforces the relevant laws).

In the Italian jurisdiction, the legal and regulatory edifice governing the domains of data protection, privacy, and cybersecurity manifests itself as a stratified and dynamically evolving system, wherein supranational norms emanating from the European Union are received and implemented through a complex interweaving of national legislative measures, sector-specific regulations, and administrative enforcement mechanisms. At the apex of this normative architecture resides Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR"), which exerts direct effect within the Italian legal order and is complemented, specified, and, where permitted, derogated by Legislative Decree No. 196 of 30 June 2003, as amended by Legislative Decree No. 101 of 10 August 2018 (hereinafter the "Italian Privacy Code").

Pursuant to the GDPR, personal data are defined in Article 4(1) as "any information relating to an identified or identifiable natural person," and the principles governing the lawful processing thereof—such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality—are enshrined in Article 5. The Italian Privacy Code, in alignment with these overarching principles, introduces provisions of particular relevance to national contexts, including norms on health data processing, journalistic activities, public interest archiving, and employment-related data. It also establishes the Italian supervisory authority, the *Garante per la Protezione dei Dati Personali* (hereinafter, also, "Garante"), vested with investigatory, corrective, advisory, and authorisation powers under both Article 58 GDPR and Article 144 et seq. of the Italian Code.

From a cybersecurity perspective, the legislative corpus has undergone a profound and unprecedented transformation following the transposition of Directive (EU) 2022/2555 ("NIS2 Directive") via Legislative Decree No. 138 of 4 September 2024. Said Decree repealed the former Legislative Decree No. 65/2018, thus abrogating the prior transposition of Directive (EU) 2016/1148 ("NIS1"), and ushered in a more expansive and vertically integrated regulatory model. The current legislative configuration delineates a dichotomy between "essential" and "important" entities (as per Articles 3 and 6 of Legislative Decree No. 138/2024), both of which are subject to ex ante registration with the national competent authority—the *Agenzia per la Cybersicurezza Nazionale* (ACN)—and must implement proportionate cybersecurity risk-management measures and incident notification obligations pursuant to Articles 18 to 23 of the same Decree, in conformity with the Implementing Regulation (EU) 2024/2690.

Furthermore, the ACN operates as the central authority for both policy coordination and operational enforcement in matters of national cybersecurity, as formalised by Decree-Law No. 82 of 14 June 2021, converted with amendments into Law No. 109 of 4 August 2021. Said instrument institutionalised the National Cybersecurity Perimeter, defined by DPCM No. 131/2020 and subsequently elaborated upon by ACN determinations, imposing stringent obligations on strategic operators in sectors such as energy, finance, health, digital infrastructure, and defence, with respect to ICT asset registration, risk assessments, and security-by-design requirements.

As regards the financial sector, Regulation (EU) 2022/2554 ("Digital Operational Resilience Act" or "DORA") has introduced a sui generis regulatory apparatus focused on ensuring the ICT resilience of financial entities. DORA is directly applicable and is operationally supported by Delegated Regulations (EU) 2024/1773 and 2024/1774, which specify technical standards on third-party risk management and simplified risk governance, respectively. Supervision under DORA is exercised by national competent authorities in coordination with the European Supervisory Authorities (EBA, ESMA, EIOPA), and, where applicable, with the ACN in light of the strategic relevance of ICT service providers.

Moreover, the corpus of cybersecurity and privacy obligations is enriched by the applicability of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards—expressly recognised under Annex I of the Commission Implementing Regulation 2024/2690—as best practices for the implementation of cybersecurity risk management frameworks. These standards are

extensively incorporated into the ACN's technical and organisational security models, including the "Modello Nazionale delle Misure Minime di Sicurezza," which functions as a de facto national cybersecurity baseline.

In addition, the Italian data protection framework encompasses sectoral laws such as Legislative Decree No. 82/2005 ("Codice dell'Amministrazione Digitale") and Legislative Decree No. 259/2003 ("Codice delle Comunicazioni Elettroniche"), which impose obligations on public administrations and telecommunications operators, respectively, with particular regard to data integrity, authentication, and lawful interception.

Finally, oversight is exercised by a polycentric constellation of authorities: the *Garante* for matters of data protection; the ACN for cybersecurity strategy, certification, and incident response; AGCOM for media and communications; Banca d'Italia and CONSOB for financial supervision under DORA; and, where relevant, the judiciary for ex post enforcement and sanctioning, including criminal liability under Articles 167–170-bis of the Privacy Code and under the Penal Code for cybercrimes pursuant to Law No. 48/2008.

Such is the intricate and multifocal configuration of the Italian legal order in the domain of data protection and cybersecurity, wherein constitutional guarantees (Articles 2, 13, 14, 15, and 21 of the Italian Constitution) intersect with European law imperatives, culminating in a normative mosaic that is simultaneously supranationally integrated and domestically plural.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

The biennium 2025–2026 shall likely witness a further intensification of the regulatory and institutional consolidation process already set in motion by the successive waves of European legislative intervention in the realms of data protection, privacy, and cybersecurity. In the Italian jurisdiction, several transformative trajectories—legislative, interpretative, and enforcement-related—may be identified as sources of imminent juridical metamorphosis.

Foremost among these evolutions stands the full operability of Directive (EU) 2022/2555 (NIS2), whose transposition into the domestic legal order has been effectuated through Legislative Decree No. 138 of 4 September 2024. The Italian National Cybersecurity Agency (*Agenzia per la Cybersicurezza Nazionale*, ACN), in its capacity as the designated competent authority, has already initiated the progressive activation of the digital platform for registration, compliance verification, and incident reporting, as prescribed under Articles 7 and 40 of the said Decree and detailed in the Determination ACN No. 38565/2024. Entities falling within the NIS2 scope shall face escalating obligations in the course of 2025, especially as the implementing decrees and delegated acts—including Commission Implementing Regulation (EU) 2024/2690—are rendered enforceable with regard to technical and organisational cybersecurity measures, supervisory protocols, and sector-specific exemptions.

Simultaneously, the Digital Operational Resilience Act (Regulation (EU) 2022/2554, "DORA"), which became applicable across the Union as of 17 January 2025, shall begin to produce substantive effects on the financial and insurance sectors, with particular regard to operational ICT risk governance, third-party service provider scrutiny, and mandatory digital resilience testing regimes. The supervisory remit of national financial regulators such as the Bank of Italy and CONSOB shall now extend to encompass DORA compliance audits, with joint oversight responsibilities articulated in coordination with the European Supervisory Authorities and, where applicable, the ACN. Moreover, the operationalisation of Delegated Regulations (EU) 2024/1773 and 2024/1774 shall result in the incorporation of complex contractual, technical, and procedural requirements into outsourcing and risk management policies, notably concerning the use of cloud and ICT services supporting critical functions.

Parallel to these developments, it is anticipated that Italy shall elaborate further secondary legislation and technical standards aimed at implementing the European Cybersecurity Certification Framework, as established under Regulation (EU) 2019/881 ("Cybersecurity Act"). In this context, the ACN has been entrusted with the role of National Cybersecurity Certification Authority and shall likely introduce schemes harmonised with ENISA-endorsed certification initiatives, particularly in sectors such as industrial control systems, IoT devices, and cloud computing infrastructures.

From the standpoint of data protection, while no amendments to the GDPR are currently foreseen, the Italian *Garante per la Protezione dei Dati Personali* is expected to issue revised national guidelines on the processing of biometric data, algorithmic profiling, and digital workplace surveillance, in light of its recent interpretative orientations and pending judicial decisions. Additionally, the interplay between GDPR obligations and

sectoral regimes, such as those under the Italian Health Data Space initiatives or the digital identity frameworks pursuant to Regulation (EU) 2024/1183, may prompt interpretative realignments and require ad hoc compliance mechanisms.

Notably, the imminent formal adoption and implementation of the Artificial Intelligence Act (AI Act), whose final text was politically agreed upon in December 2023 and is scheduled to enter into force during 2025 with phased obligations, shall pose significant compliance challenges. The AI Act, though distinct from the GDPR, introduces a complementary regulatory corpus that imposes ex ante risk assessments, conformity procedures, and post-market monitoring, particularly for high-risk AI systems that intersect with personal data processing. The Italian legislator shall thus be required to designate competent market surveillance authorities and adapt existing data protection impact assessment (DPIA) frameworks to account for AI-specific risk vectors.

It is also worth observing that the enforcement environment is undergoing a tangible shift towards a more assertive, multi-agency model. The *Garante* has intensified its inspectional and sanctioning activities, especially with respect to large-scale data brokers and digital platforms, while the ACN has augmented its proactive role through threat intelligence dissemination, vulnerability notification duties, and ex officio supervision under the national cybersecurity perimeter regime. The Italian judiciary, moreover, is increasingly engaged in the adjudication of disputes involving cross-border data transfers, data subject rights enforcement, and algorithmic discrimination.

In conclusion, the Italian regulatory landscape in data protection, privacy, and cybersecurity is poised to enter a phase of dense normative stratification and heightened operational complexity, marked by the full enactment of NIS2 and DORA, the emergence of AI and digital identity regulations, and an assertive posture by supervisory authorities, all of which shall collectively redefine the compliance and governance architectures of public and private sector actors.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

In the Italian jurisdiction, while the general architecture of data protection law as embodied by GDPR does not predicate the lawfulness of personal data processing on the prior acquisition of a formal licence or registration—having, in fact, repealed the notification and authorisation system that characterised the antecedent Directive 95/46/EC—recent legislative innovations in the domain of cybersecurity have (re)introduced obligatory mechanisms of entity registration, reporting, and regulatory alignment, particularly under the aegis of the transposed Directive (EU) 2022/2555 (NIS2) and the national cybersecurity perimeter framework.

Specifically, pursuant to Legislative Decree No. 138 of 4 September 2024, implementing the NIS2 Directive, entities falling within the categories of "essential entities" and "important entities," as defined under Articles 3 and 6 thereof, are under a non-derogable legal duty to register with the competent national authority—the *Agenzia per la Cybersicurezza Nazionale* (ACN). Article 7, paragraph 1, of said Decree mandates that entities within scope must register or update their registration through the digital platform provided by the ACN, furnishing the authority with extensive information on their organisational, operational, and infrastructural attributes, including sector classification, legal status, point of contact, and network and information system dependencies. This obligation is further operationalised by the Determination of the Director-General of the ACN No. 38565/2024, which prescribes the technical modalities and procedural requirements governing the platform interface, timelines for compliance, and the designation of liaison officers.

Entities subject to the national cybersecurity perimeter—established under Decree-Law No. 105 of 21 September 2019, converted by Law No. 133 of 18 November 2019—must undergo an additional registration process entailing the submission of exhaustive asset inventories, ICT supply chain documentation, and security policy declarations. These obligations, though overlapping with the NIS2 framework, are not coextensive, and failure to reconcile the two registration regimes may expose the entity to administrative sanctions and disqualify it from accessing public procurement or strategic infrastructure roles.

Exemptions from such registration duties are narrowly construed. Under Article 6(3) of Legislative Decree No. 138/2024, micro and small enterprises, as defined by Commission Recommendation 2003/361/EC, are generally excluded from the scope of NIS2, save where such entities operate in critical sectors such as energy, transport, banking, healthcare, and public electronic communications, or where they are designated by the competent authority on the basis of a risk-based assessment. Similarly, entities subject to alternative but

equivalent regulatory obligations—such as credit institutions governed by the Single Supervisory Mechanism—may benefit from procedural harmonisation but are not exempted in substance from the obligation to register.

Failure to register or to maintain an up-to-date registration may trigger a cascade of adverse legal consequences. Under Article 31 of Legislative Decree No. 138/2024, the ACN is empowered to impose administrative pecuniary sanctions proportional to the entity's annual turnover, ranging up to ten million euros or 2% of global annual revenue, in addition to issuing binding orders to cease operations, undertake remedial action, or suspend services deemed to pose a cybersecurity risk. Repeated or egregious non-compliance may further result in public notification of breaches, reputational damage, and disqualification from eligibility for government subsidies or public-private partnership schemes involving critical infrastructure.

Moreover, in the specific case of Digital Operational Resilience Act (DORA) compliance, although no ex ante licence is required, financial entities must notify their competent authorities of the use of critical ICT third-party service providers and submit periodic registers of contractual arrangements. Non-compliance may entail supervisory measures, including fines and mandatory audits, administered by national financial regulators in collaboration with the Joint Oversight Teams to be established under Article 31 of DORA.

Therefore, although the GDPR framework eschews registration formalities, the cybersecurity domain—in both general and sectoral permutations—has definitively reinstated a paradigm of prior identification and ongoing supervision, wherein registration operates not as a mere formal prerequisite but as a foundational vector for risk-based regulatory governance, with non-compliance bearing not only pecuniary but also strategic and reputational ramifications.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

Under the Italian legal order, the definitional architecture of data protection is substantively and formally harmonised with the provisions of GDPR, which is directly applicable in the domestic legal system and complemented by the Italian Privacy Code, which integrates and adapts the GDPR provisions to the national context.

Pursuant to Article 4(1) GDPR, "personal data" are defined as "any information relating to an identified or identifiable natural person," the latter being a data subject "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." This definition is entirely transposed into the Italian Privacy Code and constitutes the foundational category upon which the edifice of data protection obligations is constructed. Neither the GDPR nor the Italian implementing legislation makes use of the term "personally identifiable information" as found in other jurisdictions, such as the United States, opting instead for a broader and more inclusive construct that encompasses any direct or indirect linkability to a natural person.

The notion of "special categories of personal data," colloquially referred to as "sensitive data," is enshrined in Article 9(1) GDPR and expressly includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as 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. In the Italian framework, these categories receive additional specification in Articles 2-sexies and 2-septies of the Italian Privacy Code, which further delineate the conditions under which such data may be lawfully processed, including the requirement for national or Union law to provide appropriate safeguards and the necessity for prior authorisation by the Garante in specific sectors, such as scientific research or employment contexts.

Other key definitional terms within the GDPR, and thereby within the Italian legal system, include:

- "Data controller" (*titolare del trattamento*), as defined in Article 4(7) GDPR, refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Italian

jurisprudence has developed nuanced interpretative criteria to ascertain controller status, particularly in cases involving joint controllership or ambiguous delegations of decision-making power.

- "Data processor" (*responsabile del trattamento*), under Article 4(8) GDPR, denotes the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Article 28 GDPR prescribes the content of the binding contractual relationship between controller and processor, while the Italian Privacy Code specifies, in Article 2-quaterdecies, additional provisions regarding sub-processing and liability.
- "Data subject" (*interessato*), pursuant to Article 4(1) GDPR, is the identified or identifiable natural person to whom the personal data relate. This status endows the individual with a panoply of rights—access, rectification, erasure, restriction, portability, objection, and the right not to be subject to automated decision-making—all of which have been operationalised and expanded upon in Italian regulatory and jurisprudential practice.
- "Processing" (*trattamento*) is defined in Article 4(2) GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means," and includes collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, erasure or destruction. This capacious definition is mirrored verbatim in Article 4(1)(a) of the Italian Privacy Code.
- "Filing system" (*archivio*), as per Article 4(6) GDPR, refers to any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed.

In addition to the above, Italian law incorporates further distinctions, such as the figure of the *responsabile della protezione dei dati* (Data Protection Officer), whose designation, tasks, and qualifications are governed by Articles 37 to 39 GDPR and further detailed in Garante guidelines. Moreover, the Italian Privacy Code retains the figure of the *incaricato del trattamento* (formerly designated as "data handler" under pre-GDPR law), now largely obsolete, but still occasionally referenced in certain public sector contexts and collective agreements.

Thus, the Italian legislative and interpretative approach to definitional matters under data protection law is characterised by faithful adherence to the GDPR's lexicon, enriched by sectoral elaborations and interpretive guidance issued by the Garante, which collectively ensure a high degree of legal certainty, terminological consistency, and regulatory harmonisation within the European data protection acquis.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

In the Italian legal system, the processing of personal data is governed by the fundamental principles codified in Article 5 of GDPR, which constitutes the directly applicable normative foundation for all data processing operations within the jurisdiction. These principles, being of axiological and operational significance, are further entrenched and operationalised by the Italian Privacy Code, as well as by interpretative guidelines of the Garante.

First and foremost among the cardinal principles is that of **lawfulness, fairness and transparency**, which mandates that all data processing be grounded in one of the legal bases exhaustively enumerated in Article 6 GDPR and that the data subject be informed, in a manner that is intelligible, accessible and comprehensive, of the circumstances, purposes, and consequences of such processing. In accordance with Articles 13 and 14 GDPR, controllers are under an obligation to provide privacy notices specifying inter alia the identity and contact details of the controller and, where applicable, of the data protection officer, the purposes and legal basis of the processing, the recipients of the data, the period for which the data will be stored, and the data subject's rights.

The principle of **purpose limitation** dictates that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This is particularly reinforced in the Italian context by sectoral provisions that prohibit the reuse of data acquired for administrative or employment purposes for profiling, marketing, or investigatory ends without an independent legal basis and proportionality assessment.

Closely linked is the principle of **data minimisation**, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Garante has, on multiple occasions, enjoined data controllers from deploying overly intrusive forms of surveillance or

monitoring (notably in workplace contexts), reaffirming that the principle of necessity must always be interpreted restrictively and substantiated by a demonstrable risk analysis.

The **accuracy** of personal data is another inviolable precept, entailing that data must be kept up to date and that every reasonable step must be taken to ensure that inaccurate data are rectified or erased without delay. Italian jurisprudence has underscored this obligation particularly in the domain of creditworthiness assessments and reputational databases, where erroneous or outdated information can generate substantial legal and economic prejudice.

The **storage limitation** principle, in turn, prescribes that personal data be retained only for as long as necessary to fulfil the purposes for which they were collected. Article 5(1)(e) GDPR is echoed in Article 2-octies of the Italian Privacy Code, which imposes sector-specific retention limits—for example, in the context of traffic data retained for public security purposes (as per Legislative Decree No. 109/2008) or employment records, whose retention must comply with labour and fiscal law constraints. Controllers are thus required to implement data retention policies and, where applicable, automated deletion schedules, as confirmed by the Garante's Resolution No. 467 of 11 October 2018 on storage limitation criteria.

The principle of **integrity and confidentiality**, or security, mandates that personal data be processed in a manner ensuring appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32 GDPR finds expression in the Italian legal order through mandatory adoption of risk-based security protocols, with compliance frequently benchmarked against ISO/IEC 27001 and the national minimum security measures model (*Modello Nazionale delle Misure Minime di Sicurezza*), as endorsed by the ACN.

Lastly, the principle of **accountability**, enshrined in Article 5(2) GDPR, places the onus on the controller to not only comply with all the aforementioned principles, but also to be able to demonstrate such compliance at all times. This encompasses obligations to maintain records of processing activities pursuant to Article 30 GDPR, to conduct data protection impact assessments under Article 35 GDPR when processing is likely to result in high risk, and to consult the supervisory authority where residual risks remain.

It is also imperative to recall that the legal bases for processing under Article 6 GDPR include consent, contract performance, compliance with legal obligations, protection of vital interests, public interest tasks, and legitimate interest pursued by the controller. The Italian *Garante*, consistent with EDPB interpretations, has issued detailed guidance on the validity of consent (including its revocability and granularity), the limits of legitimate interest, and the inapplicability of certain bases—e.g., legitimate interest—in scenarios involving high-risk profiling or vulnerable data subjects.

Accordingly, the principle-based architecture of data processing in Italy is not merely declaratory but is rendered operational through a multiplicity of statutory obligations, sector-specific constraints, and interpretative standards, thereby ensuring that the processing of personal data is not only formally legitimate but substantively respectful of the dignity, freedom, and informational self-determination of the individual.

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

An exhaustive examination of the requisites concerning the validity, scope, and formal characteristics of consent under Italian data protection law reveals a normative and interpretative construction rigorously anchored to the GDPR, as directly applicable and hierarchically superior, yet integrated and operationalised domestically by the Italian Privacy Code.

Pursuant to Article 6(1)(a) GDPR, the consent of the data subject constitutes a lawful basis for the processing of personal data only insofar as it is "freely given, specific, informed and unambiguous". Article 4(11) GDPR further defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". This dual definitional framework precludes, ab origine, the admissibility of consent that is presumed, passive, implicit, or derived by omission or inertia.

The Italian Supervisory Authority has consistently reaffirmed, notably through Provvedimento generale in materia di consenso del 24 February 2005 and

subsequent interpretative guidelines (e.g., Guidelines on cookies and other tracking tools, June 2021), the necessity for consent to be unequivocal, granular, and expressed through a positive action. Hence, so-called "opt-out" mechanisms or the inclusion of pre-ticked boxes are unequivocally deemed incompatible with the GDPR standard.

In terms of the formal requirements governing consent, the GDPR and the Privacy Code jointly impose a series of constraints which inhibit the possibility of integrating consent within broader legal instruments—such as general terms and conditions of service—without a distinct and highlighted indication. Article 7(2) GDPR specifically prescribes that "if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language". The failure to observe such segmentation renders the consent not binding.

Further, Article 7(4) GDPR prohibits the so-called "bundled consent" where "the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". This entails, as per consolidated jurisprudence and Garante's case law, that the request for consent must be articulated per processing purpose and that each consent must be revocable individually, at any time and without prejudice to the lawfulness of the processing based on consent prior to its withdrawal.

A particular attention must be reserved to processing operations based on consent involving special categories of personal data under Article 9(2)(a) GDPR, as well as data concerning minors, where Article 8 GDPR applies. In the latter case, in the Italian jurisdiction, the minimum age threshold for valid digital consent remains fixed at 14 years, as established under Article 2-quinquies of the Privacy Code. Below such age, the consent must be provided or authorised by the holder of parental responsibility.

Moreover, under Italian law, the administration of consent must be auditable and demonstrable by the data controller pursuant to Article 7(1) GDPR. This imposes not only the adoption of technical and organisational measures to record, archive and retrieve proof of the consent, but also the burden of demonstrating that the consent was obtained in accordance with the aforementioned substantive and procedural conditions.

No derogation or simplification is permitted on the basis of the nature of the controller (public or private) nor of the data (ordinary or pseudonymised), save for specific regulatory bases under Article 6(1)(b)-(f) GDPR which may obviate the necessity of consent altogether.

In summation, within the Italian legal landscape as shaped by EU primary and secondary legislation and authoritatively interpreted by the Garante, consent may not be presumed, deduced, implied, or bundled, and must be obtained through an autonomous, granular and revocable manifestation of will. Any deviation therefrom exposes the controller to both administrative sanctions pursuant to Article 83 GDPR and invalidation of the underlying processing operation for lack of lawful basis.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

The processing of particular categories of personal data within the Italian jurisdiction is subject to a layered regime of heightened legal safeguards, procedural constraints, and sectoral prohibitions, articulated primarily through the combined application of GDPR and the Italian Privacy Code. This framework operates in tandem with the jurisprudence of the Italian Supervisory Authority and relevant acts of soft law, thereby creating a substantively dense and procedurally stringent corpus for the lawful handling of sensitive data.

Pursuant to Article 9(1) GDPR, the processing of "special categories of personal data" is prohibited unless one of the exceptions enumerated in Article 9(2) applies. These special categories include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic and biometric data for the purpose of uniquely identifying a natural person; data concerning health; and data concerning a natural person's sex life or sexual orientation. In the Italian legal system, these provisions are further elaborated under Article 2-septies of the Italian Privacy Code, which mandates that the processing of such data be permitted solely when authorised by a specific provision of Union or national law or when expressly authorised by the Garante, upon adoption of appropriate safeguards.

Health data processing is subject to one of the most stringent regulatory regimes. Article 2-septies and Article

75 et seq. of the Italian Privacy Code delineate the contexts within which health data may be processed, including for purposes of preventive or occupational medicine, medical diagnosis, provision of health or social care, or management of health systems, subject always to professional secrecy obligations. Where processing is carried out by public entities such as health authorities or regional administrations, the Garante has further issued binding authorisations and codes of conduct, notably the *Codice di deontologia per il trattamento dei dati personali effettuato per scopi statistici e scientifici*, which establishes additional duties concerning pseudonymisation, data minimisation, and access controls.

With respect to children's data, the Italian legislator has exercised the national margin of discretion provided under Article 8 GDPR by establishing the age threshold for valid digital consent at 14 years, as opposed to the general age of 16 contemplated under the Regulation. This rule is codified in Article 2-quinquies of the Italian Privacy Code, which mandates parental or guardian consent for the processing of data of children below this age. The Garante has issued multiple enforcement actions in cases involving educational platforms, online gaming, and social media operators for failure to implement adequate age-verification mechanisms and for unlawful profiling of minors. Additional obligations arise under Law No. 71 of 29 May 2017 on cyberbullying, which requires the expeditious deletion of defamatory or harmful online content involving minors, in coordination with the Garante.

In terms of biometric and genetic data, Article 2-septies of the Italian Privacy Code requires, in addition to a valid legal basis, that processing be preceded by a data protection impact assessment (DPIA) under Article 35 GDPR and, in certain cases, be subject to prior consultation with the Garante pursuant to Article 36 GDPR. The processing of such data for access control or time management purposes in employment contexts has been consistently restricted by the Garante, particularly where less intrusive alternatives are available, thereby reaffirming the principle of proportionality.

Furthermore, the Italian legal system incorporates absolute prohibitions on the processing of certain types of data unless permitted by law. For example, under Article 2-decies of the Italian Privacy Code, data disclosing a person's membership in political parties, trade unions, religious associations, or philosophical organisations may not be disseminated to third parties absent a compelling legal basis and explicit consent. Similarly, Article 8 of Law No. 300 of 20 May 1970 (the "Statuto dei Lavoratori") prohibits the employer from processing data pertaining to the political, religious, or trade union opinions of employees, even with their consent, except where strictly necessary and in compliance with collective agreements or national laws.

Particular scrutiny also applies to the use of AI and algorithmic profiling when applied to special categories of data. While Article 22 GDPR prohibits automated decision-making that produces legal effects or similarly significant consequences, the Italian Privacy Code and Garante guidance underscore that where such processing involves sensitive data, the burden of justification and safeguard implementation is exponentially heightened. This includes the adoption of human oversight mechanisms, transparency of the logic involved, and avenues for contestation.

Accordingly, the Italian regime governing the processing of special categories of personal data is characterised by a convergence of absolute prohibitions, conditional authorisations, enhanced accountability mechanisms, and sector-specific constraints, all geared towards the preservation of individual dignity, non-discrimination, and informational self-determination in accordance with the principles enshrined in Articles 2, 3, and 13 of the Italian Constitution and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

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

An exhaustive analysis of the derogatory provisions, exemptions, exclusions, and limitations embedded within the data protection laws applicable to the Italian jurisdiction necessitates a nuanced exegesis that takes into consideration both the general regulatory corpus delineated by GDPR and the domestic implementing measures enacted pursuant to the Italian Privacy Code, with further integration drawn from regulatory and interpretative contributions of the Italian Supervisory Authority.

Pursuant to Article 23 GDPR, Member States retain the faculty to restrict—through legislative measures—the scope of data subjects' rights and of the obligations incumbent upon data controllers and processors, provided that such restrictions respect the essence of fundamental rights and freedoms and are necessary and proportionate in a democratic society. In this regard, the Italian legislator has availed itself of such faculty through

the enactment of the Italian Privacy Code, which introduces a compendium of derogations and limitations with specific regard to national interests of elevated constitutional significance.

Among the principal domains wherein such derogations are operationalised, it is imperative to consider the exemptions concerning journalistic purposes and freedom of expression and information. In particular, Article 136 et seq. of the Italian Privacy Code establishes that the application of several provisions of the GDPR—including, inter alia, those relating to the lawfulness of processing, the right to erasure, and the right to restriction of processing—may be restricted where personal data are processed for journalistic purposes or for the purpose of academic, artistic, or literary expression. Such restrictions, however, are admissible solely in so far as they are necessary to reconcile the right to personal data protection with the freedom of expression as protected under Article 21 of the Italian Constitution.

Further derogatory provisions are delineated in the context of processing for scientific or historical research purposes or for statistical purposes, in alignment with Article 89 GDPR. The Italian Privacy Code supplements the GDPR by affirming that personal data processed for such purposes may be subjected to limitations on data subjects' rights, including those enshrined in Articles 15 to 22 GDPR, where the exercise of such rights would render impossible or seriously impair the achievement of the research objectives. It must be noted, however, that such processing remains subject to appropriate safeguards, including pseudonymisation and minimisation principles, as expressly prescribed by the Garante's general authorisations.

In the domain of employment relationships, the Italian Privacy Code introduces further delimitations. In particular, pursuant to Article 113 and 114 of the Codice, the exercise of data subjects' rights may be curtailed to ensure compliance with obligations or to exercise specific rights of the data controller or of the data subject in the field of employment law and social protection, in consonance with Article 88 GDPR. Additionally, data processing activities carried out for whistleblowing purposes are subject to specific derogations in terms of transparency obligations, as codified in recent national legislation on the protection of whistleblowers.

The Italian data protection framework also contains exemptions applicable in the context of processing activities carried out by public authorities for purposes connected to criminal investigations, prosecution, national security, and public order. In these instances, Articles 2-undeicies and 2-duodecies of the Italian Privacy Code introduce substantial limitations to the exercise of data subjects' rights, grounded upon the imperative of safeguarding overriding public interests. In particular, the exercise of the rights set forth in Articles 15 to 22 GDPR may be restricted where such restriction constitutes a necessary and proportionate measure to protect national security, defence, public security, or the prevention, investigation, detection and prosecution of criminal offences.

Moreover, the scope of application of the GDPR and the Italian Privacy Code is circumscribed by the general principle of territoriality and material scope. Accordingly, processing performed by natural persons in the course of a purely personal or household activity falls outside the ambit of data protection law, in conformity with Article 2(2)(c) GDPR and Article 2(2) of the Italian Privacy Code.

Finally, sector-specific legislation continues to provide further layers of exemptions and special regimes, particularly in the banking, insurance, telecommunications, and public administration sectors, whereby the Garante has adopted sectoral authorisations, codes of conduct, and other instruments delineating the contours of lawful derogation, most notably under the aegis of Article 40 and 41 GDPR.

In sum, the Italian legal order has exercised the discretionary margin conferred by the GDPR to articulate a composite array of exclusions and derogations, which, while rooted in supranational principles, find their operational specificity within the national constitutional, legislative, and regulatory framework, always subject to the proportionality and necessity tests imposed by the jurisprudence of the Court of Justice of the European Union and the Constitutional Court of the Italian Republic.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

The Italian legal system, as harmonised with the GDPR, unequivocally requires the performance of a data protection impact assessment (DPIA) in all those circumstances where processing operations, "in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, are likely to result in a high risk to the rights and freedoms of natural persons" (cf. Article 35(1) GDPR). This imperative finds its domestic corollary in Article 5(2)

of the Italian Privacy Code, which incorporates by reference the GDPR obligations and delegates to the Italian Supervisory Authority the authority to specify, through general measures, those processing operations deemed intrinsically high-risk and thus mandatorily subject to such assessment.

In fulfilment of the faculty granted under Article 35(4) GDPR, the Garante adopted its *Provvedimento contenente l'elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, par. 4, del Regolamento (UE) 2016/679*, on 11 October 2018. The measure identifies several categories of processing requiring DPIA *ab initio*, including but not limited to: systematic monitoring of publicly accessible areas on a large scale; processing of biometric data to uniquely identify individuals; profiling activities with legal effects or similarly significant consequences; large-scale processing of sensitive data under Article 9 GDPR or data relating to criminal convictions under Article 10; and interconnections or comparisons of datasets held by different data controllers.

The substantive and procedural architecture of the DPIA is set forth under Article 35(7) GDPR, which mandates that the assessment shall contain at least: a systematic description of the envisaged processing operations and the purposes of the processing; an assessment of the necessity and proportionality of the processing in relation to those purposes; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks, including safeguards and security measures to ensure the protection of personal data and to demonstrate compliance with the Regulation.

In addition to the general obligation to conduct DPIAs where risks are high, the Garante's own guidance—such as the *Linee guida in materia di valutazione d'impatto sulla protezione dei dati (DPIA)* adopted in alignment with the WP29 Guidelines—urges the controller to embrace a proactive stance, conducting impact assessments even where not strictly mandatory, whenever the processing operation introduces significant novelties in scope, scale, or technological complexity, or implicates systematic monitoring or surveillance.

From a methodological standpoint, the DPIA must be conducted prior to the commencement of the processing and should be conceived as a dynamic instrument, subject to periodic review throughout the lifecycle of the processing activity. It is incumbent upon the controller, pursuant to Article 24 GDPR, to ensure that the DPIA is properly documented and that it reflects an objective and traceable risk management approach. To this end, controllers typically rely on structured methodologies—often aligned with ISO/IEC 29134:2017 or national standards validated by ENISA—and employ both qualitative and quantitative metrics for risk identification, evaluation, and mitigation planning.

In situations where the DPIA identifies residual risks that cannot be sufficiently mitigated by the envisaged safeguards, Article 36 GDPR imposes a prior consultation obligation with the competent supervisory authority, which, in the Italian jurisdiction, remains exclusively the Garante. The latter retains the power to issue binding opinions, impose additional conditions, or prohibit the processing altogether, thereby ensuring that high-risk processing does not proceed without adequate protective guarantees.

Thus, in the Italian legal order, the DPIA represents not merely a compliance requirement, but an emblematic manifestation of the accountability principle under Article 5(2) GDPR, operationalised through a rigorous, pre-emptive, and documented assessment mechanism, essential to the lawful exercise of personal data processing where high risks are implicated.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

Within the Italian jurisdiction, the processing of personal data is not only governed by binding legislative instruments such as GDPR and the Italian Privacy Code, but is also complemented and operationalised by a sophisticated corpus of soft law instruments, prominently including *codici di condotta* (codes of conduct) and *regole deontologiche* (ethical rules), which assume quasi-normative force under Articles 40 and 41 GDPR and the corresponding provisions of national law.

In accordance with Article 2-quater of the *Italian Privacy Code*, the Italian Supervisory Authority may endorse sector-specific codes of conduct proposed by trade associations or professional bodies, following a public consultation and compatibility assessment with the GDPR. These codes, once approved, become binding upon adherents and may form the basis for the imposition of corrective measures and sanctions in cases of non-compliance. Moreover, Article 2-quaterdecies of the *Italian Privacy Code* permits the Garante to formulate binding ethical rules in certain sectors, particularly those involving sensitive data or complex risk profiles.

Among the most significant instruments currently in force is the *Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*, which regulates the processing of personal data in the context of academic, biomedical, and social research. This code, adopted under Article 20 of the prior data protection regime and retained under the transitional provisions of Article 21 of Legislative Decree No. 101/2018, imposes stringent safeguards regarding data minimisation, pseudonymisation, ethical review, and data subject information rights.

In the domain of health data, particularly sensitive in nature and regulated under Articles 9 and 89 GDPR as well as Article 2-septies of the *Italian Privacy Code*, the Garante has promulgated various ethical rules and guidelines. Notable among these is the *Regolamento recante prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs. 10 agosto 2018, n. 101*, which outlines permissible health data processing scenarios and delineates mandatory safeguards including limited data retention, restricted access, and logging of disclosures.

Regarding children's data, the Garante has not adopted a standalone code of conduct under Articles 40–41 GDPR but has issued multiple resolutions and interpretative guidelines delineating lawful processing parameters. Particularly relevant is the interpretative application of Article 8 GDPR via Article 2-quinquies of the *Italian Privacy Code*, which sets the age of digital consent at 14 years and requires mechanisms to verify parental responsibility below this threshold. In 2020, the Garante published the *Linee guida sull'utilizzo dei dati personali in ambito scolastico*, which provide an operational matrix for data processing within educational institutions, covering video surveillance, publication of students' images, digital platforms, and parental consent protocols.

In the employment context, the Garante's *Regole deontologiche relative al trattamento di dati personali nell'ambito dei rapporti di lavoro*, originally adopted under the pre-GDPR regime and still applied by analogy, remain influential. They proscribe disproportionate monitoring, limit data retention for disciplinary purposes, and require transparency in the deployment of biometric systems and geolocation technologies.

Furthermore, the Italian legal order recognises the binding character of the *Regole deontologiche per il trattamento dei dati personali a fini di informazione commerciale* and the *Codice di condotta per i sistemi di informazioni creditizie*, both of which regulate data flows within the financial and credit sectors, impose obligations of data accuracy, and provide for the establishment of ADR mechanisms in case of disputes.

Lastly, under the GDPR's encouragement of accountability via voluntary adherence to codes of conduct, several sectoral codes have been proposed and are undergoing evaluation by the Garante and the European Data Protection Board (EDPB), including in the domains of cloud service provision, telemedicine, and scientific research involving biobanking.

In summation, the Italian system reflects a normatively dense and operationally nuanced reliance on sector-specific codes of conduct and deontological rules, which serve to articulate granular compliance standards, mitigate sectoral risks, and provide interpretative clarity, all while reinforcing the foundational principles of proportionality, necessity, and transparency that pervade the broader data protection acquis.

11. Are organisations required to maintain any 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 prevailing legal regime applicable in the Italian jurisdiction, the obligation incumbent upon data controllers and data processors to maintain detailed records of processing activities, as codified under Article 30 of GDPR, finds full and direct application. This provision, which does not admit national derogation or modulation, operates in tandem with the interpretative and prescriptive framework furnished by the Italian Supervisory Authority, whose guidelines and inspectional protocols confer upon said obligation an essential role within the organisational accountability architecture of the processing entity.

Pursuant to Article 30(1) GDPR, each controller—and, where applicable, the controller's representative—is obliged to maintain a written or electronic record of processing activities under its responsibility, delineating inter alia the purposes of processing, categories of data subjects and of personal data, categories of recipients, including transfers to third countries or international organisations, envisaged time limits for erasure, and a general description of technical and organisational security measures. Analogously, processors are subject to the mirroring obligation set forth under Article 30(2) GDPR, concerning processing activities carried out on behalf of a controller.

Although Article 30(5) GDPR exempts undertakings or organisations employing fewer than 250 persons, such

exemption is strictly circumscribed and does not extend to processing likely to result in a risk to the rights and freedoms of data subjects, or processing that is not occasional, or includes special categories of data pursuant to Article 9(1) or personal data relating to criminal convictions and offences as per Article 10. In practical terms, such exemption proves to be of limited utility, as the vast majority of structured processing operations, including those carried out by microenterprises, fall within the scope of mandatory record-keeping.

In the Italian context, the Garante, through its inspection activities and public pronouncements, has consistently reaffirmed the centrality of the Article 30 record—referred to in domestic practice as "registro delle attività di trattamento"—as an instrument of proactive accountability, transparency, and auditability. The record is not merely a descriptive document, but is required to be consistent with the entity's actual data processing architecture and integrated into its broader data protection governance framework, including the risk-based approach underlying Data Protection Impact Assessments (DPIA), the implementation of appropriate security measures, and the management of data subjects' rights.

Businesses operating within the jurisdiction typically comply with such requirement through the adoption of formalised internal documentation systems, often supported by compliance software or data governance platforms that permit structured data mapping, dynamic record updates, and audit traceability. The record is commonly integrated into the privacy management system established under ISO/IEC 27701 or within broader ISMS frameworks conforming to ISO/IEC 27001 and 27002 standards, thereby enabling harmonised documentation practices aligned with principles of data minimisation, purpose limitation, and storage limitation.

Moreover, Italian data protection practice, especially within regulated sectors such as banking, insurance, and health care, has witnessed a convergence between Article 30 records and sector-specific documentation obligations imposed by supervisory authorities, such as the Bank of Italy, IVASS, and the Ministry of Health. In such contexts, the record frequently functions as a nucleus around which orbit other compliance instruments, including records of joint controllership arrangements, processor agreements pursuant to Article 28 GDPR, and internal audit documentation regarding access controls, incident response, and training activities.

It is further to be noted that the record, while not subject to notification or prior approval, must be made available to the supervisory authority upon request. This requirement, interpreted strictly by the Garante, implies that the record must not only exist, but be complete, up-to-date, and reflective of the processing reality at the time of the authority's inspection. Failure to maintain or produce such record constitutes a serious compliance deficiency and may result in administrative fines under Article 83(4)(a) GDPR.

In conclusion, the obligation to maintain records of processing activities constitutes a cornerstone of the accountability principle enshrined in Article 5(2) GDPR and finds concrete articulation within Italian data protection law and practice as a sine qua non for any lawful and demonstrable compliance regime.

12. 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).

The normative architecture governing the retention and disposal of personal data within the Italian jurisdiction, as shaped by the GDPR and supplemented by the Italian Privacy Code, unequivocally mandates the establishment of data retention and destruction protocols, both as a direct legal obligation and as an indispensable emanation of the broader principle of accountability and lawfulness.

Pursuant to Article 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". This foundational norm enshrines the so-called *principle of storage limitation*, which requires a case-by-case assessment of the necessity and proportionality of data retention in light of the processing's original, specific, and legitimate purposes. The same provision admits the retention of data for longer periods only where such storage is required for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, provided appropriate safeguards are in place.

Article 24 GDPR, which embodies the accountability principle, and Article 25, which codifies the notion of data protection by design and by default, collectively imply the implementation of internal retention and disposal policies by the controller as demonstrative instruments of compliance. These instruments must clearly identify retention periods or criteria for each category of data processed and must foresee secure and irreversible disposal mechanisms once the retention term lapses or the processing purpose has been exhausted.

Within the Italian normative system, the Italian Supervisory Authority has consistently reaffirmed, in numerous decisions and sectoral guidelines, the obligation to adopt documented policies on data retention. Notable examples include the *Linee guida in materia di posta elettronica e Internet* (2007, updated in 2023), which require public and private employers to define and communicate clear retention timelines for logs and e-mail metadata, and the *Provvedimenti in materia di videosorveglianza*, which impose strict temporal limits—typically not exceeding 24 to 72 hours—for the retention of surveillance footage, unless specific risks justify an extension.

Additionally, the Garante's *Regole deontologiche* applicable to specific professional categories (journalists, healthcare providers, scientific researchers) stipulate minimum and maximum retention periods and impose erasure obligations where the retention no longer complies with proportionality and necessity principles.

The administrative dimension of retention obligations is further complemented by sectoral legal regimes that impose prescriptive storage terms, such as tax, labour and public procurement laws, which may require the preservation of specific documentation for periods up to ten years. In these instances, the GDPR's principle of harmonised interpretation mandates that the controller reconcile such obligations with the minimisation principle under Article 5(1)(c), employing appropriate technical and organisational safeguards to limit access and further processing.

Moreover, Recital 39 GDPR underscores the necessity of defining retention periods upfront and ensuring that data no longer necessary be either anonymised or securely erased. The secure erasure of data—whether digital or paper-based—constitutes a positive obligation arising from Article 32 GDPR (security of processing) and must be documented through technical procedures that ensure irreversibility and prevent re-identification.

From a procedural standpoint, the data disposal process must be embedded in the controller's security policies, incident response strategies, and business continuity plans. The ISO/IEC 27001:2022 and ISO/IEC 27040 standards, widely adopted by data controllers in Italy, provide methodological guidance on data sanitisation and physical destruction techniques, including data wiping, degaussing, cryptographic erasure, and physical shredding.

In conclusion, both under Union and Italian law, data retention and disposal policies are not only strongly recommended but often strictly required as operational instruments of the overarching principles of data protection. Their absence or inadequacy may constitute a breach of the controller's accountability obligations and expose the entity to administrative fines under Article 83(5) GDPR, reputational harm, and potential civil liability.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Under the Italian legal framework, consultation with the Italian Supervisory Authority is not merely discretionary but mandated under specific normative contingencies established by GDPR and the Italian Privacy Code, particularly in scenarios that entail heightened risks to the rights and freedoms of data subjects or which involve processing operations characterised by systemic complexity, opacity, or technological novelty.

The primary circumstance necessitating **mandatory prior consultation** is codified in Article 36(1) GDPR. Where a data protection impact assessment (DPIA), conducted pursuant to Article 35, indicates that the processing is likely to result in a high risk in the absence of measures taken by the controller to mitigate such risk, the controller is required to consult the supervisory authority before proceeding. This applies, inter alia, to large-scale profiling, use of biometric or genetic data, systematic monitoring of publicly accessible areas, or use of new technologies not previously subjected to regulatory vetting. Article 36(5) GDPR obliges the controller to provide the authority with the DPIA, a description of the intended processing, and measures envisaged to protect data subjects.

In the Italian jurisdiction, the *Garante* has adopted **Guidelines on DPIAs and high-risk processing activities**, which include an indicative list of processing operations subject to mandatory consultation. These include, inter alia, scoring systems used in recruitment, e-recruitment platforms employing automated decision-making, and the large-scale deployment of facial recognition systems. Failure to conduct prior consultation where required may result in administrative sanctions under Article 83(4)(a) GDPR and corresponding provisions of the *Italian Privacy Code*.

Moreover, **consultation is also required in cases of processing carried out on behalf of a public authority** for reasons of substantial public interest, particularly where the legal basis for processing is Article 9(2)(g) GDPR in conjunction with Article 2-sexies of the *Italian Privacy Code*. In such scenarios, consultation with the *Garante* ensures that adequate legal and technical safeguards

have been embedded in the processing design, especially in domains such as public health surveillance, biometric identification for access to public services, or large-scale databases for law enforcement.

Beyond mandatory prior consultation, the *Garante* may be consulted **voluntarily** by controllers or processors where legal uncertainty prevails or where the envisaged processing is novel or intersects with conflicting regulatory regimes, such as financial supervision, labour law, or public procurement. This is consistent with the preventive function attributed to the *Garante* under Article 154 of the *Italian Privacy Code*, which empowers the Authority to issue interpretative opinions and non-binding recommendations.

Further, under Italian law and practice, certain processing operations require **prior authorisation by the *Garante***, particularly where sensitive data are involved and processing falls outside the derogations permitted under Article 9(2) GDPR. Examples include processing for genetic research, use of health data by private entities for secondary purposes, or cross-border transfers of data to third countries absent an adequacy decision or binding corporate rules.

Additionally, consultation is expected in the context of **data breach notifications** under Article 33(1) GDPR. Although not a consultation in the strict sense, the notification to the *Garante* of a personal data breach within 72 hours—where the breach is likely to result in a risk to the rights and freedoms of natural persons—frequently initiates a regulatory dialogue wherein the authority may request supplementary documentation, remedial action plans, or impose ex officio corrective measures under Article 58 GDPR.

Equally, Italian law imposes consultation duties in the context of **public sector digitalisation**. Pursuant to Article 2-sexiesdecies of the *Italian Privacy Code*, public entities are obliged to consult the *Garante* when introducing or significantly modifying information systems or databases that process personal data, particularly where interconnection with other administrative databases is envisaged.

Lastly, it is customary—and increasingly expected—for data controllers participating in **certification schemes, adherence to codes of conduct**, or **cross-border processing activities** involving multiple jurisdictions to engage with the *Garante* either directly or via the consistency mechanism under Chapter VII GDPR, coordinated by the EPDB.

In conclusion, the duty to consult the *Garante* pervades multiple strata of the Italian data protection system, encompassing not only mandatory ex ante procedural requirements in high-risk processing scenarios but also constituting a broader mechanism for regulatory risk management and normative alignment, reflecting the Authority's institutional role as both enforcer and interlocutor in the governance of informational self-determination.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

In the Italian legal order, the obligation to designate a Data Protection Officer (hereinafter, "DPO") arises from the direct applicability of Article 37 et seq. of GDPR, and is further entrenched through domestic interpretative praxis developed by the Italian Supervisory Authority, which has issued specific guidelines clarifying the material scope and practical implementation of such obligation. The legislative landscape, moreover, extends beyond the figure of the DPO, encompassing parallel designations within cybersecurity governance, such as the Chief Information Security Officer (hereinafter, "CISO"), particularly in sectors subject to the Perimetro di Sicurezza Nazionale Cibernetica and the obligations deriving from the recepimento of Directive (EU) 2022/2555 (NIS2).

Pursuant to Article 37(1) GDPR, the designation of a DPO is mandatory where the processing is carried out by a public authority or body (except for courts acting in their judicial capacity), where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or where the core activities consist of processing on a large scale of special categories of data or data relating to criminal convictions and offences. These thresholds, though seemingly abstract, have been concretely interpreted by the Garante, whose inspectional activity has clarified that the DPO must be designated not only in cases of manifest applicability, but also where prudential risk assessment indicates the presence of latent qualifying criteria.

The legal responsibilities of the DPO are set out in Article 39 GDPR and are, by their nature, both advisory and supervisory. The DPO is entrusted with the duty to inform and advise the controller or processor and their employees of their obligations under data protection law,

to monitor compliance with the GDPR and with national provisions, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations. Moreover, the DPO is tasked with providing advice regarding data protection impact assessments pursuant to Article 35 GDPR, and with cooperating with the supervisory authority, acting as the point of contact on issues relating to processing.

The DPO must be designated on the basis of professional qualities, and in particular, expert knowledge of data protection law and practices. The position must be supported by functional independence, protection against dismissal or penalisation, and adequate resources. In the Italian context, these requirements have been reaffirmed by the Garante through its deliberation no. 146 of 13 June 2019, which emphasises that the DPO may be either internal or external to the organisation, provided the independence and conflict-of-interest requirements are respected.

Simultaneously, the cybersecurity normative corpus, notably as delineated by the Legislative Decree no. 105 of 21 September 2019 (converted with amendments by Law no. 133 of 18 November 2019), and more recently by Legislative Decree no. 138 of 4 September 2024 implementing Directive (EU) 2022/2555, requires the designation of roles functionally analogous to the DPO, but with a more pronounced technical-operational focus. Entities included within the Perimetro di Sicurezza Nazionale Cibernetica are obligated to appoint a "Referente per la Sicurezza Cibernetica", a role which often coincides with the CISO, tasked with the coordination and implementation of cybersecurity measures, the supervision of incident response procedures, and direct interfacing with the Agenzia per la Cybersicurezza Nazionale (ACN) and the CSIRT Italia.

Such figure, although not provided for under the GDPR, is now a de facto indispensable counterpart to the DPO in contexts where the interrelation between personal data protection and information security is structurally inextricable. Where personal data constitute assets within the critical information infrastructure, the operational convergence between the DPO and CISO becomes imperative to guarantee coherence between legal compliance, risk management, and technical implementation.

In practice, Italian organisations often opt for a multidisciplinary team or an integrated governance structure whereby the DPO operates in coordination with the CISO, the Privacy Officer, and the Legal and Compliance functions. This collaborative architecture is particularly evident in sectors regulated by sectoral authorities such as Banca d'Italia, IVASS, and AGID, which impose stringent cybersecurity and data governance obligations.

In conclusion, Italian data protection laws, in faithful implementation of the GDPR and in synergy with national cybersecurity requirements, impose a stratified and functionally nuanced regime of mandatory roles, whose effectiveness depends not only on formal designation, but on the substantive capacity to influence processing operations, monitor compliance, and engage with supervisory authorities in a legally autonomous and operationally integrated manner.

15. 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) or recommendation(s).

The corpus of data protection norms currently in force within the Italian jurisdiction, as articulated in GDPR and further detailed by the Italian Privacy Code, imposes—both directly and by necessary implication—a categorical obligation upon data controllers and processors to ensure the adequate training of personnel in matters pertaining to personal data protection.

The juridical basis for such obligation is to be found primarily in Article 32(4) GDPR, which explicitly provides that "any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law". The operational corollary of this provision is the ineludible necessity that such authorised individuals be adequately trained to comprehend and execute such instructions in compliance with the legal requirements governing data processing.

In parallel, Article 24(1) GDPR requires that the controller "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation". In this context, the notion of "organisational measures" has been consistently interpreted by the Italian Supervisory Authority and by the prevailing European data protection doctrine as encompassing the periodic training of personnel authorised to process data, particularly where the processing operations involve high-risk activities, sensitive data categories, or large-scale processing.

This interpretation is corroborated by multiple formal acts

of the Garante, including the *Linee guida in materia di misure di sicurezza* (2001), the *Provvedimento generale in tema di amministratori di sistema* (2008, updated in 2018), and more recently by the *Vademecum per i Responsabili della Protezione dei Dati* (2020), all of which explicitly delineate employee training as an indispensable component of the minimum compliance architecture. In particular, the Garante has highlighted that training must be tailored, documented, and recurrent, and must encompass both substantive data protection principles and concrete operational instructions concerning security protocols, incident reporting, access controls, and confidentiality duties.

Moreover, the Italian national cybersecurity framework, particularly as codified in Legislative Decree No. 105 of 21 September 2019 on the national cybersecurity perimeter, as well as the more recent Legislative Decree No. 138 of 4 September 2024 transposing Directive (EU) 2022/2555 (NIS2 Directive), require that public and private operators of critical and essential services implement training and awareness programmes as part of their broader risk management and incident preparedness strategies. The *Modello Nazionale per l'Implementazione delle Misure di Sicurezza per il PSNC* (2023), adopted by the Agenzia per la Cybersicurezza Nazionale (ACN), explicitly includes personnel training as a mandatory control within the governance and security domains.

Under the principles of data protection by design and by default (Article 25 GDPR), the controller must ensure that all employees who, by reason of their functions, are involved in the processing of personal data, are not only formally authorised pursuant to Article 29 GDPR but also instructed through appropriate training initiatives commensurate with their roles, access levels, and operational exposure to data processing.

It is also pertinent to observe that the obligation of training extends to Data Protection Officers (DPOs), who, pursuant to Article 39(1)(b) GDPR, are required to "monitor compliance with this Regulation… including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations". Consequently, the DPO is charged with both the oversight and the orchestration of training programmes, which must be documented in a manner that permits ex post auditability and accountability in accordance with Article 5(2) GDPR.

In sum, the Italian data protection legal order does not merely recommend but unequivocally mandates the adoption of structured and recurring training for all personnel involved in personal data processing activities. The failure to implement such training may not only constitute a breach of Article 32 GDPR, thereby exposing the data controller to significant administrative sanctions under Article 83(4)(a) GDPR, but may also amount to gross negligence in the event of data breaches, with consequential implications in civil, labour, and criminal law domains.

16. 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).

The Italian data protection regime, being structurally integrated within the legal framework established by GDPR, imposes an unequivocal and non-derogable obligation upon data controllers to provide comprehensive notice to data subjects concerning the modalities, purposes, and implications of personal data processing operations. Such obligation is enshrined in Articles 13 and 14 GDPR and receives full domestic enforceability within the Italian legal order without need of transpositional enactment, although it is complemented by interpretative guidance issued by the Italian Supervisory Authority pursuant to Article 154 of the Italian Privacy Code.

The notification requirement varies in its operational articulation depending upon whether the personal data are collected directly from the data subject or acquired from third-party sources. In the former case, Article 13 GDPR mandates that the controller provide the information at the time of collection; in the latter case, Article 14 GDPR requires provision of the same within a reasonable period, not exceeding one month, or at the time of first communication with the data subject, whichever occurs first.

The notification must encompass, in an intelligible and accessible form, at minimum: the identity and contact details of the controller and, where applicable, the data protection officer; the purposes of processing and its legal basis; the categories of personal data concerned (where not obtained directly); the recipients or categories of recipients of the data; the envisaged data retention period; the rights of the data subject including access, rectification, erasure, restriction, portability, objection, and the right not to be subject to automated decision-making; the existence of any intention to transfer data to a third country and the legal mechanism for such transfer; and the right to lodge a complaint with a supervisory authority.

In accordance with Article 12 GDPR and the guidance of the EPDB, the information must be conveyed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. For online services, this has resulted in the widespread deployment of multilayered privacy policies, wherein an initial short notice summarises key information and hyperlinks to more detailed disclosures. The *Garante* has explicitly endorsed this practice, provided the core information is not rendered obscure by excessive abstraction or hypertextual fragmentation.

Particular emphasis is placed upon the principle of transparency, and failure to fulfil the notification duty is deemed not merely a procedural irregularity but a substantive infringement of the data subject's rights to information and autonomy, subject to administrative fines under Article 83(5)(b) GDPR and, in egregious cases, reputational and contractual liability.

Furthermore, pursuant to Article 2-ter of the *Italian Privacy Code*, if the processing is based on a legal obligation or public interest task under Article 6(1)(c) or (e) GDPR, and such legal basis is grounded in Italian or Union law, the data subject must be expressly informed of the provision of law or the administrative measure constituting the legal basis, as well as the specific tasks or functions carried out by the controller.

Exceptions to the duty to provide notice, under Article 14(5) GDPR, are interpreted restrictively and apply only in circumstances where provision proves impossible or would involve disproportionate effort, or where data are subject to professional secrecy, judicial privilege, or national security limitations. Even in such instances, the *Garante* requires that controllers adopt compensatory transparency measures, such as public disclosure on institutional websites or via data protection registers.

For specific sectors—such as employment, health, and education—the *Garante* has issued detailed templates and best practice guidelines regarding the structure and content of privacy notices, which are expected to be strictly adhered to. For example, in the employment domain, the *Garante* mandates that employees be informed of the presence and scope of any monitoring tools, the legal basis for such monitoring, and the duration of data retention, in accordance with Article 4 of Law No. 300/1970 (Statuto dei Lavoratori).

In sum, the obligation to provide notice to data subjects constitutes a cornerstone of the Italian data protection framework, operationalising the constitutional principle of *informational self-determination* and serving as a foundational safeguard for the exercise of data subject rights. Non-compliance is not merely a technical failure but a material breach of the controller's duty of loyalty and transparency, attracting supervisory scrutiny and potential sanctions.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

The delineation of distinct normative obligations, liabilities, and functional responsibilities between data controllers and data processors constitutes one of the cardinal principles underpinning both GDPR and its implementation within the Italian legal order. The distinction—enshrined with marked clarity and operability within Articles 4(7) and 4(8), as well as Chapters IV and V of the GDPR—is both formally received and substantively reinforced through the Italian Privacy Code, and through consolidated interpretative praxis developed by the Italian Supervisory Authority.

A data controller is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Conversely, a data processor processes personal data on behalf of the controller, under the latter's documented instructions, unless otherwise required by Union or Member State law. This bifurcation establishes a clear line of demarcation with respect to decision-making autonomy and legal accountability.

The implications of such differentiation are profound and multifaceted. Controllers bear the primary burden of accountability under Article 5(2) GDPR and are directly responsible for ensuring compliance with the core principles governing the processing of personal data, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality. They must also implement appropriate technical and organisational measures in accordance with the principle of data protection by design and by default (Article 25 GDPR), maintain records of processing activities (Article 30(1)), conduct Data Protection Impact Assessments where appropriate (Article 35), and ensure the lawfulness of data transfers to third countries (Chapter V GDPR).

Processors, while ostensibly subordinate in their functional role, are nonetheless bound by an autonomous set of obligations under Article 28 GDPR and other

provisions. They must not engage another processor without prior specific or general written authorisation from the controller; they must ensure that persons authorised to process the data are subject to confidentiality undertakings; and they must implement security measures as per Article 32 GDPR. Furthermore, processors are now directly liable under Article 82 GDPR for damages caused by processing activities where they have not complied with their legal obligations or acted outside or contrary to the lawful instructions of the controller.

Italian data protection law reinforces such division by requiring that the relationship between controller and processor be governed by a binding legal act—typically a data processing agreement—which must specify, inter alia, the subject matter, duration, nature, and purposes of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. The Garante, through specific inspection guidelines and enforcement actions, has elucidated that the absence or inadequacy of such agreement constitutes a material non-compliance and exposes both parties to administrative sanctions.

A further implication arises in the context of joint controllership, where two or more controllers jointly determine the purposes and means of processing. Under Article 26 GDPR, they must, by means of an arrangement, transparently determine their respective responsibilities, including as regards the exercise of data subjects' rights and the provision of information as required by Articles 13 and 14 GDPR. The Garante has clarified that such arrangements must not merely exist pro forma, but must be effectively implemented and demonstrable to the supervisory authority upon request.

In administrative and judicial practice, liability is apportioned in accordance with the degree of autonomy and compliance of each actor. Controllers are presumed primarily liable, whereas processors are liable in their own right for breach of contractual or regulatory duties. Furthermore, processors may not invoke lack of control over the purposes and means of processing as a blanket shield from liability, particularly in cases where they have exercised de facto control or made substantive decisions without authorisation.

In conclusion, the legal framework operative within the Italian jurisdiction not only recognises but substantively operationalises the distinction between controllers and processors, attributing to each a defined perimeter of duties, liabilities, and procedural obligations, the violation of which may entail not only administrative sanctions under Article 83 GDPR, but also civil liability for damages, reputational harm, and—where applicable—criminal consequences under ancillary national provisions.

18. 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 or any similar terms defined?

The Italian legal framework, situated within the supranational edifice established by GDPR, articulates a multifaceted and restrictive regime governing monitoring activities, automated decision-making, profiling operations, and the utilisation of tracking technologies—such as cookies—predicated upon a composite interplay of substantive safeguards, procedural prerequisites, and sectoral norms, all of which converge to preserve the inviolability of individual autonomy and informational self-determination.

Within the lexicon of EU data protection law, “profiling” is defined under Article 4(4) GDPR as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." “Automated decision-making" in turn pertains, pursuant to Article 22 GDPR, to any decision “based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects him or her."

Such processing modalities are not per se prohibited under Italian law; however, they are enveloped within a regime of heightened scrutiny and conditional legitimacy. Article 22(1) GDPR enunciates a general prohibition, from which three exceptions emerge: (a) where the decision is necessary for entering into or performance of a contract; (b) where authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms; and (c) where it is based on the data subject's explicit consent. The Italian Privacy Code, at Article 2-octies, confirms and reiterates such conditions, whilst imposing supplementary safeguards in cases involving special categories of data, minors, or vulnerable data subjects.

In circumstances where automated decision-making or profiling is legally permissible, Article 22(3) GDPR

mandates the implementation of appropriate safeguards, which at minimum must include the right to obtain human intervention, to express one's point of view, and to contest the decision. The Italian Supervisory Authority, in its interpretative practice, has underscored the obligation to provide clear and intelligible information about the logic involved, the significance, and the envisaged consequences of such processing (cf. *Linee guida su processi decisionali automatizzati e profilazione*).

With respect to monitoring activities—particularly within the employment context—the Italian legal order imposes a stricter regime deriving not only from GDPR principles but also from Article 4 of Law No. 300 of 20 May 1970 (Statuto dei Lavoratori), which forbids the use of audio-visual or other equipment for the purpose of monitoring employees' activity unless specific trade union agreements or labour inspectorate authorisations are obtained. Such constraints apply equally to the deployment of biometric systems, GPS-based tracking, and other ICT tools capable of indirectly monitoring work performance.

Turning to tracking technologies such as cookies, the regulatory schema is principally governed by Article 122 of the Privacy Code, which transposes Article 5(3) of Directive 2002/58/EC ("ePrivacy Directive"). Under such provision, the storage of information or the access to information already stored in the terminal equipment of a user is permitted only if the user has given prior informed consent, upon receipt of a comprehensive and clearly visible notice. This consent requirement is waived solely for "technical cookies" strictly necessary to carry out the transmission of a communication over an electronic communications network or to provide an information society service explicitly requested by the user.

The Garante, through its *Linee guida cookie e altri strumenti di tracciamento* (10 June 2021), has further specified that consent must be freely given, specific, informed, and unambiguous, and that it cannot be obtained through implicit mechanisms (e.g., continued navigation), nor can it be bundled with other purposes. The same guidelines prohibit the use of pre-ticked boxes or cookie walls that impede access to content absent consent. Moreover, the controller is required to implement a granular cookie banner that allows the user to selectively authorise each category of cookies, accompanied by a user-friendly consent management interface.

In synthesis, the Italian jurisdiction imposes a restrictive and compliance-intensive regime upon monitoring, profiling, automated decision-making and the use of tracking technologies, grounded in a legal tradition that privileges the primacy of individual rights over algorithmic opacity and surveillance capitalism. The lawful execution of such processing operations demands an elevated standard of transparency, granular consent, and algorithmic accountability, failing which the data controller incurs not only administrative liability under Article 83 GDPR, but may also be exposed to judicial remedies, class actions, and injunctive measures imposed by the Garante.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

The Italian legal regime governing targeted advertising and behavioural advertising is embedded within the broader matrix of data protection, privacy, and electronic communications law, drawing its primary legal foundations from GDPR and Directive 2002/58/EC ("ePrivacy Directive"), as implemented by the Italian Privacy Code. Although neither the GDPR nor the *Italian Privacy Code* provide a statutory definition of "targeted advertising" or "behavioural advertising," these practices are conceptually understood—pursuant to the interpretative guidance of the Italian Supervisory Authority and the EPDB —as encompassing the automated monitoring of data subjects' online activities and the subsequent profiling thereof for the purpose of delivering personalised advertisements.

Under the GDPR, such advertising falls squarely within the scope of "profiling" as defined in Article 4(4), which denotes "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person." When profiling is employed for marketing purposes, particularly in conjunction with automated decision-making under Article 22 GDPR, it is considered to pose elevated risks to the data subject's rights and freedoms, thereby triggering a cascade of enhanced obligations, including explicit consent under Article 6(1)(a), transparency under Articles 13 and 14, and the right to object under Article 21(2).

The *Garante* has, through multiple resolutions and sectoral investigations, established that the deployment of tracking technologies—such as cookies, device fingerprinting, SDKs, and pixels—for behavioural advertising purposes requires the data subject's prior, free, specific, informed and unambiguous consent, in conformity with the GDPR and Article 122 of the *Italian Privacy Code*, which transposes Article 5(3) of the ePrivacy Directive. This consent must be obtained through a positive affirmative act, typically via a consent

management platform (CMP) or cookie banner, and cannot be presumed through silence, pre-ticked boxes, or continued navigation.

The Garante's *Guidelines on Cookies and Other Tracking Tools* (Resolution No. 231 of 10 June 2021) impose a number of formal and substantive requirements on consent collection mechanisms, including the prohibition of dark patterns, the obligation to provide an "accept all/reject all" function at the first layer, and the duty to facilitate the revocation of consent as easily as it was given. Moreover, the use of third-party cookies or tracking tools for marketing purposes requires that both the deploying and receiving entities be identified as joint controllers under Article 26 GDPR, unless the third party processes data under its own exclusive purposes, in which case a distinct legal basis and notice obligation applies.

It is further established that the processing of data for behavioural advertising may not be based on the legitimate interests of the controller, particularly where the data subject is a child, or where large-scale tracking is carried out in a covert or intrusive manner. The Garante has consistently ruled that such practices fail the balancing test under Recital 47 GDPR and Article 6(1)(f), especially in view of the asymmetry of information and bargaining power that characterises the digital advertising ecosystem.

Additional constraints apply to the combination of offline and online data sets, particularly when derived from loyalty programmes, data brokers, or third-party aggregators. In such cases, the Garante has required controllers to conduct data protection impact assessments (DPIAs) under Article 35 GDPR, and to implement robust safeguards including pseudonymisation, minimisation, and audit trails. Controllers who engage in cross-device tracking or geo-targeted behavioural advertising are likewise expected to notify users of such practices in their privacy notices, with granular explanation of profiling logic, legal basis, and consequences.

Particular vigilance is imposed on advertising directed at minors. In accordance with Article 2-quinquies of the *Italian Privacy Code* and the Garante's guidance on digital consent, profiling for marketing purposes of data subjects under the age of 14 is categorically prohibited absent verified parental consent, and advertising platforms are expected to implement effective age-verification and content-restriction mechanisms.

The *Garante* has also imposed multimillion-euro administrative fines on multinational digital platforms for infringing behavioural advertising rules, particularly in cases where consent was bundled with terms of service, or where dark patterns undermined the user's freedom of choice. Such enforcement reflects the Italian authority's active participation in the cross-border enforcement mechanisms of the GDPR under the auspices of the EDPB, including the one-stop-shop mechanism and coordinated decisions under Article 65.

Therefore, the Italian regulatory environment imposes significant legal and operational constraints on targeted and behavioural advertising, treating them not merely as ancillary marketing techniques but as high-risk processing operations requiring scrupulous adherence to data protection principles, rigorous consent protocols, and full transparency. Any deviation from these norms constitutes a material infringement subject to corrective and punitive measures under both national and Union law.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

The Italian legal system, as integrated within the broader framework of European Union data protection law, does not explicitly adopt the terminology of "sale" of personal data, nor does it provide a statutory definition of such term in the manner characteristic of other jurisdictions such as California's Consumer Privacy Act (CCPA). Nevertheless, the alienation, transfer, or exchange of personal data for pecuniary or other forms of consideration is addressed through a stringent matrix of substantive and procedural constraints embedded within GDPR, as directly applicable and further specified by the Italian Privacy Code.

Within this legal architecture, any operation involving the communication or dissemination of personal data, including transfers to third parties for economic purposes, is subject to the foundational principles of lawfulness, fairness, and transparency enshrined in Article 5(1) GDPR. The transfer of personal data for consideration, or its inclusion within commercial transactions such as data brokerage, constitutes a processing operation which must be grounded in one of the lawful bases exhaustively enumerated under Article 6 GDPR. In the absence of a lawful basis—such as explicit consent under Article 6(1)(a) or the necessity of processing for the performance of a contract under Article 6(1)(b)—any monetisation or exchange of personal data is deemed unlawful.

Moreover, where the processing pertains to special categories of data pursuant to Article 9 GDPR, the threshold is even more restrictive, requiring the existence of a specific derogatory condition, such as explicit consent or a substantial public interest grounded in Union or Member State law. The Italian Supervisory Authority has consistently held that economic exploitation of sensitive data, particularly for marketing, profiling, or commercial enrichment purposes, is permissible only under conditions of heightened transparency and prior informed, specific, and granular consent.

While Italian and European law abstain from defining "sale" per se, the notion is functionally subsumed under broader categories of "communication" or "disclosure" to third parties, both of which are tightly regulated. In this context, the Garante has clarified, inter alia through its decision no. 161 of 22 April 2021, that the transfer of databases or contact lists to third parties—even within intra-group contexts—requires a lawful basis and must be accompanied by complete and comprehensible disclosure to data subjects pursuant to Articles 13 and 14 GDPR.

Particular caution applies to scenarios involving behavioural advertising, real-time bidding (RTB), or programmatic advertising models wherein data are circulated in digital marketplaces. Such models have come under critical scrutiny by the EPDB and are deemed lawful only if implemented with adequate safeguards, including explicit consent, DPIAs, and algorithmic accountability.

Furthermore, Italian law prohibits any processing of personal data for purposes incompatible with those for which the data were originally collected, unless permitted under Article 6(4) GDPR, subject to a compatibility test and supplementary safeguards. Thus, the commodification of personal data—where it departs from the initial lawful purpose—may result in a breach of purpose limitation and trigger sanctions under Article 83 GDPR.

From a contractual standpoint, the inclusion of personal data as an asset in mergers, acquisitions, or asset deals is likewise conditioned upon the compliance with the GDPR. The Garante has stipulated that the acquirer assumes the obligations of the controller and must notify data subjects of the change in control and ensure continuity of lawful processing. In particular, any retroactive broadening of processing purposes or use for monetisation post-transfer would necessitate fresh consent.

In sum, while the Italian legal system refrains from articulating a formal definition of "sale" of personal data, the concept is subsumed within a legally complex network of restrictions grounded in the GDPR's core principles. The economic valorisation of personal data, absent full compliance with those principles and without demonstrable lawful basis, is categorically impermissible and exposes the actor to administrative sanctions, reputational damage, and potential litigation.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

The Italian legal regime governing direct marketing communications—including by means of telephone calls, SMS, email, and analogous electronic communications—reflects a structured and prohibitive orientation, anchored both in supranational instruments, primarily Directive 2002/58/EC ("ePrivacy Directive"), and in the Italian Privacy Code, as well as the interpretative corpus developed by the Italian Supervisory Authority.

At the core of this regime lies Article 130 of the Privacy Code, which enshrines the dual model of consent-based and opt-out marketing, depending on the nature of the channel used and the identity of the data subject. For marketing communications conveyed via automated means—specifically, emails, SMS, MMS, faxes, automated calling systems, push notifications, and other similar technologies—the principle of prior, specific, informed and freely given consent (*opt-in*) is mandatory. This requirement applies regardless of whether the communication is aimed at consumers or professionals, and it cannot be circumvented by general terms and conditions or bundled consent declarations.

The definition of "direct marketing" within the Italian data protection doctrine corresponds to any communication—whether for commercial, promotional or fundraising purposes—made by a controller or on its behalf, that is directed to identified or identifiable individuals, and which involves the processing of their personal data. The term encompasses not only advertising per se but also newsletters, offers, invitations, surveys and market research, where these are intended to influence purchasing behaviour or elicit economic responses.

An important derogation to the prior consent requirement is recognised under Article 130(4) of the Privacy Code—the so-called *soft opt-in*—which permits the sending of electronic marketing messages to existing

customers where the controller has acquired their email coordinates in the context of a prior sale of a product or service, and the communication pertains to goods or services similar to those already purchased. This exception, however, is conditional upon the data subject being adequately informed at the time of data collection and afforded a clear and facile opportunity to object, both at the point of initial collection and in each subsequent communication.

As regards traditional telephone marketing, a distinct opt-out regime is applicable to numbers registered in the *Registro Pubblico delle Opposizioni* (Public Register of Objections), which was reformed by Presidential Decree No. 26 of 27 January 2022 and is now extended to all publicly available or directory-listed numbers, both fixed and mobile. Article 130(3-bis) of the Privacy Code prohibits the use of such numbers for marketing unless the user has not enrolled in the Register or has expressly consented to being contacted. Furthermore, operators must identify themselves, disclose the name of the entity on whose behalf the call is made, and inform the data subject of the right to object and of how to exercise it.

The Garante has issued extensive guidance on the unlawful practices associated with so-called "wild telemarketing", including *Provvedimenti generali* against operators engaging in calls without verifiable consent, or relying on data obtained through opaque lead generation or affiliate marketing schemes. In such contexts, the onus of proof lies entirely with the controller, which must demonstrate that consent was lawfully obtained, specific to the promotional purpose, and not vitiated by coercion, deception, or lack of transparency.

Moreover, Article 21 of GDPR reinforces the individual's right to object, at any time and without charge, to processing for direct marketing purposes, including profiling to the extent it is related to such marketing. The exercise of this right triggers an immediate cessation obligation upon the controller, and any further communication may constitute an infringement punishable under Article 83(5) GDPR.

In addition to administrative sanctions, violations of direct marketing rules may also entail civil liability pursuant to Article 82 GDPR and Article 15 of the Privacy Code, with potential damages for unlawful processing, as well as reputational consequences and possible criminal exposure where deceit, falsification or identity misuse is involved (e.g., spoofing, unauthorised number masking).

In conclusion, the Italian data protection framework imposes a robustly restrictive regime on direct marketing practices, grounded in the primacy of prior consent, the enforceability of opt-out mechanisms, and the transparency of data provenance. Controllers must structure their marketing strategies in strict adherence to these provisions, subject to ongoing oversight by the Garante and judicial scrutiny upon data subject complaint.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

In the Italian legal system, the processing of biometric data—encompassing, inter alia, facial recognition technologies—falls within a highly restrictive regulatory perimeter, governed primarily by GDPR and the Italian Privacy Code. This regime is supplemented by extensive interpretative guidance and enforcement practice issued by the Italian Supervisory Authority, whose jurisprudence has consistently advocated a precautionary and risk-averse approach to biometric data processing, especially in public spaces and employment contexts.

Pursuant to Article 4(14) GDPR, **"biometric data"** are defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." This definition is mirrored in the *Italian Privacy Code*, which, under Article 2-septies, prescribes that the processing of such data may be carried out solely where authorised by Union or Member State law, accompanied by appropriate safeguards and, where applicable, subject to prior authorisation by the *Garante*.

In this context, **facial recognition** qualifies as a biometric processing operation to the extent that it involves the mathematical extraction and comparison of facial features for identification or authentication purposes. Accordingly, any deployment of facial recognition systems—whether in public surveillance, workplace access control, educational monitoring, or commercial customer tracking—must be treated as processing of special categories of personal data under Article 9 GDPR, and is presumptively prohibited unless one of the strict exceptions under Article 9(2) applies.

The Italian *Garante* has repeatedly emphasised that **explicit consent**, as per Article 9(2)(a), is generally not a sufficient legal basis when the data subject is in a position of subordination or dependence (e.g., employee, student, or user of a monopoly service), as the voluntariness of consent would be vitiated. Similarly,

reliance on the legitimate interests of the controller under Article 6(1)(f) is categorically excluded for processing operations that involve biometric data for uniquely identifying natural persons.

In accordance with Article 35 GDPR, **a data protection impact assessment (DPIA)** is mandatory prior to the commencement of any biometric data processing, particularly where the processing is systematic, large-scale, or conducted in publicly accessible areas. The *Garante* has issued a list of processing operations requiring DPIA, which explicitly includes facial recognition and biometric identification technologies, and has, in multiple decisions, required controllers to demonstrate that such processing is strictly necessary, proportionate, and cannot be replaced by less intrusive means.

Moreover, the *Garante* has prohibited or limited various implementations of biometric systems. For instance, in Decision No. 513 of 2020, it sanctioned a municipality for the unlawful deployment of facial recognition cameras in schools, finding that no adequate legal basis had been established and that fundamental rights had been disproportionately restricted. Similar restrictions have been imposed in the context of access control systems in workplaces and gyms, where fingerprint or facial recognition devices were deemed unnecessary in light of available alternatives such as RFID badges.

Italian law also provides for **sector-specific prohibitions**. Under Article 4 of Law No. 300/1970 (Statuto dei Lavoratori), the use of equipment for the remote monitoring of employees is prohibited unless justified by organisational needs and authorised by trade unions or labour authorities. The Garante has interpreted biometric access systems as potentially infringing this provision and has thus required prior consultation or authorisation.

Furthermore, with the forthcoming application of the **Artificial Intelligence Act** (politically agreed upon at the EU level in December 2023 and set to become applicable in a phased manner from 2025 onwards), the regulation of facial recognition and biometric categorisation systems shall become even more restrictive. The AI Act classifies **real-time remote biometric identification in publicly accessible spaces** by law enforcement authorities as a "high-risk" or even "prohibited" AI use case, save for strictly delineated exceptions grounded in substantial public interest, such as prevention of terrorism or serious crime. Italy shall be required to transpose these provisions into its internal administrative and oversight structures, with probable involvement of both the Garante and a newly designated national AI authority.

In conclusion, the processing of biometric data—and facial recognition in particular—is subject in Italy to a dense matrix of prohibitions, conditional authorisations, and procedural safeguards, all of which converge toward the principle that such processing must be narrowly tailored, demonstrably necessary, and accompanied by robust guarantees of transparency, accountability, and data subject rights. The prevailing doctrinal and regulatory orientation is one of prudence and restraint, reflecting the potentially irreversible impact of biometric surveillance on dignity, autonomy, and privacy in the digital age.

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

Within the Italian legal system, the regulatory treatment of artificial intelligence (hereinafter, "AI") and machine learning (hereinafter, "ML") systems in relation to personal data processing is currently situated at the intersection of general data protection law, primarily the GDPR, and emergent European-level legislative initiatives, most notably the Artificial Intelligence Act (hereinafter, "AI Act"), which—at the time of this writing in 2025—has been formally adopted but is undergoing progressive implementation. Italy, through the Italian Supervisory Authority and its institutional involvement in the EPDB, has embraced an interpretative approach that imposes rigorous obligations upon controllers and processors engaging in AI-mediated processing of personal data, pending the full operationalisation of the AI Act.

Under the GDPR, several provisions bear directly upon AI systems insofar as they involve the automated processing of personal data. Article 22 GDPR prohibits decisions based solely on automated processing, including profiling, which produce legal effects concerning the data subject or similarly significantly affect him or her, unless one of the exceptions in Article 22(2) applies. Italian doctrine and the Garante have interpreted this provision broadly to encompass AI-based determinations in credit scoring, recruitment, insurance underwriting, and risk prediction, requiring human intervention and meaningful review mechanisms to avert automated decision-making bans.

The principles of transparency and fairness under Articles 5(1)(a), 12, 13, and 14 GDPR are of paramount relevance in the AI context. Controllers must disclose the logic involved in automated decision-making, as well as the significance and envisaged consequences of such processing for the data subject. This obligation is particularly challenging where black-box algorithms or

opaque ML models are employed. The Garante has issued guidance underscoring the necessity of algorithmic explainability, accountability, and auditability, especially when the output of AI systems is used to determine eligibility or access to services.

Moreover, data minimisation (Article 5(1)(c)) and purpose limitation (Article 5(1)(b)) restrict the deployment of AI systems that indiscriminately ingest vast datasets, especially when trained on data repurposed from original contexts without proper legal basis or consent. In particular, the Garante has cautioned against the use of scraped personal data from online sources to train generative AI models, warning that such practices are likely incompatible with GDPR obligations unless lawful grounds are clearly established and data subjects' rights are guaranteed.

The Italian framework imposes specific scrutiny in relation to special categories of personal data processed through AI, particularly where biometric, genetic, or health data are involved. Such processing is subject to the stringent conditions of Article 9 GDPR and national implementing measures, including the need for explicit consent or a substantial public interest enshrined in law. This is especially pertinent in the use of AI in facial recognition, emotion detection, and behavioural analytics, where the Garante has issued restrictive interpretations aligned with EDPB recommendations.

Italy's adherence to the Perimetro di Sicurezza Nazionale Cibernetica and to the Directive (EU) 2022/2555 (NIS2 Directive), implemented domestically by Legislative Decree no. 138 of 4 September 2024, implies additional obligations for critical operators deploying AI systems, particularly in cybersecurity and incident prevention. Entities within the Perimetro are required to conduct risk assessments of AI components, ensure traceability of decisions, and notify the Agenzia per la Cybersicurezza Nazionale (ACN) of vulnerabilities in AI tools embedded in essential services.

With the recent promulgation of the AI Act—Regulation (EU) 2024/865—the Italian legal order is now compelled to ensure alignment with a harmonised horizontal framework for AI, categorising systems into unacceptable, high-risk, limited-risk, and minimal-risk classes. High-risk AI systems, including those used in employment, law enforcement, and critical infrastructure, are subject to extensive conformity assessments, human oversight obligations, and post-market monitoring. Italy, through its national market surveillance authority yet to be formally designated, shall be responsible for supervising AI Act compliance. Controllers deploying AI systems in personal data processing contexts must now concurrently fulfil GDPR and AI Act duties, including the performance of data protection impact assessments (Article 35 GDPR) and ex ante fundamental rights impact assessments under the AI Act.

In synthesis, Italian data protection law, while not yet equipped with a codified national AI statute, engages AI systems through the existing GDPR regime, enhanced by the interpretative elaboration of the Garante and the forthcoming binding obligations under the AI Act. The coalescence of these normative layers mandates that AI development and deployment within the jurisdiction be grounded in legality, transparency, proportionality, and data subject empowerment, with particular emphasis on risk assessment, human intervention, algorithmic fairness, and the enforceability of individual rights.

24. 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?)

The transfer of personal data from Italy to countries situated outside the territorial scope of the GDPR – that is, to third countries not deemed by the European Commission to provide an adequate level of data protection—is subject to a comprehensive regime of restrictions and safeguards as articulated under Chapter V of the GDPR and corroborated by interpretative guidance from the EPDB and the Italian Supervisory Authority.

Pursuant to Article 44 GDPR, any transfer of personal data to a third country or an international organisation may take place only if, and insofar as, the conditions laid down in the entire Chapter V are complied with by the controller and processor, including for onward transfers. The normative rationale underpinning these provisions is the safeguarding of the continuity and integrity of the level of protection guaranteed within the European Union, thereby averting the circumvention of data subject rights through extraterritorial data flows.

The primary mechanism for lawful transfer is the existence of an adequacy decision pursuant to Article 45 GDPR. Where the European Commission has recognised a third country, territory, or one or more specified sectors within it as ensuring an essentially equivalent level of protection, personal data may flow freely without additional authorisations. Such decisions currently exist,

inter alia, in favour of Andorra, Canada (commercial organisations), Japan, the United Kingdom, and, subject to limitations, the United States under the EU-U.S. Data Privacy Framework (adopted July 2023).

Absent an adequacy decision, data transfers must be underpinned by appropriate safeguards as set forth in Article 46 GDPR. The most frequently employed instrument in Italy is the Standard Contractual Clauses (SCCs) adopted by the European Commission under Decision 2021/914, which must be incorporated *in extenso* and unaltered, except for the completion of appendices and permissible supplementary clauses that do not contradict or undermine the Commission's text. Alternatively, controllers may adopt Binding Corporate Rules (BCRs) under Article 47 GDPR, which must be submitted for prior approval to the competent supervisory authority and require the cooperation of multiple entities within a corporate group.

Following the judgment of the Court of Justice of the European Union in *Schrems II* (Case C-311/18), all transfers based on SCCs or other Article 46 mechanisms must be preceded by a Transfer Impact Assessment (TIA), which evaluates the legal environment of the recipient country, with particular reference to governmental access to data and the availability of judicial redress. Where the TIA reveals that the laws of the third country may impinge upon the effectiveness of the SCCs, the controller is under a duty to implement "supplementary measures"—technical (e.g., strong encryption, pseudonymisation), contractual, or organisational—that bring the level of protection in line with EU standards.

The GDPR further provides, under Article 49, for a limited set of derogations for specific situations, such as the explicit consent of the data subject (with prior information on the risks), necessity for the performance of a contract, or important reasons of public interest. These derogations, however, are to be interpreted restrictively and cannot serve as the basis for repetitive, large-scale, or structural transfers.

It should be noted that, under Italian administrative practice, no general obligation of notification to or prior authorisation by the Garante applies where transfers are conducted under Articles 45, 46, or 47 GDPR. However, where recourse is made to Article 49 derogations in the absence of other safeguards, especially for non-occasional transfers, the controller may be required to demonstrate the adequacy and exceptional nature of such reliance, particularly in the event of a complaint or investigation.

The Garante has also issued specific guidance on data transfers to jurisdictions such as the United States, China, and Russia, and has actively intervened to block or prohibit transfers deemed incompatible with EU law, notably in the context of digital service providers and cloud-based infrastructures not affording adequate guarantees.

In operational terms, Italian businesses typically ensure compliance by implementing the SCCs into their contractual matrices, maintaining detailed records under Article 30 GDPR, conducting TIAs, and integrating transfer risk assessments within their broader data protection impact assessments (DPIAs) where high-risk processing is involved. Documentation and accountability are paramount, and compliance must be demonstrable ex post to supervisory authorities.

In conclusion, the cross-border transfer of personal data from Italy is governed by a stringent and structured legal regime, wherein transfers to third countries are permitted solely upon the existence of an adequacy finding or the deployment of robust legal and technical safeguards. The overarching objective is the preservation of the level of protection guaranteed within the Union, irrespective of the geographical relocation of the data.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

The Italian legal system, in alignment with the overarching architecture established by GDPR, imposes a complex and multifaceted regime of personal data security obligations upon controllers and processors, articulated through a risk-based, technologically adaptive, and accountability-oriented model. These obligations are codified primarily in Articles 5(1)(f) and 32 of the GDPR and further specified by the Italian Privacy Code, as well as interpretative and prescriptive acts issued by the Italian Supervisory Authority.

At the core of this normative framework lies the **principle of integrity and confidentiality**, enshrined in Article 5(1)(f) GDPR, which mandates that personal data be processed "in a manner that ensures appropriate security," including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, through the use of appropriate technical or organisational measures. This obligation is not merely aspirational but constitutes a legally enforceable duty of care, non-compliance with which exposes the controller or processor to administrative sanctions under Article 83(4)(a) GDPR.

Article 32 GDPR provides the operational blueprint for this obligation, requiring the implementation of "appropriate technical and organisational measures" to ensure a level of security commensurate with the risk. Such measures must take into account "the state of the art, the costs of implementation, the nature, scope, context and purposes of processing," and the risks to the rights and freedoms of natural persons. The Italian Supervisory Authority has interpreted this clause to mandate a contextual and dynamic assessment, whereby controllers must periodically review and update their security posture in light of evolving threats, technological developments, and changes in processing operations.

Concretely, the measures contemplated by Article 32 include, but are not limited to: pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the capacity to restore availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Within the Italian jurisdiction, these general requirements are bolstered by sectoral specifications and best practice models. Particularly noteworthy is the *Modello Nazionale delle Misure Minime di Sicurezza*, developed under the auspices of the *Agenzia per la Cybersicurezza Nazionale* (ACN), which delineates a matrix of mandatory and recommended controls for public sector bodies and critical infrastructure operators, harmonised with international standards such as ISO/IEC 27001:2022 and ISO/IEC 27002:2022. This model categorises controls according to NIST-like functions (Identify, Protect, Detect, Respond, Recover) and specifies granular requirements in areas such as asset management, access control, incident response, and cryptographic governance.

Furthermore, Article 33 of the GDPR, as complemented by national guidance, imposes an obligation to notify the Italian Supervisory Authority of any personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the risk is high, Article 34 GDPR mandates direct communication to the data subjects concerned, unless an exception applies. The Italian Supervisory Authority has issued specific templates, interpretative guides, and risk classification criteria to standardise and operationalise these reporting duties.

Additionally, Article 28(3)(c) GDPR mandates that processors, in their contractual arrangements with controllers, undertake to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the protection of data subjects' rights. Failure to include such clauses renders the processing relationship non-compliant and exposes both parties to regulatory scrutiny.

For processing involving **special categories of personal data**, as per Article 9 GDPR, or **large-scale profiling and monitoring**, as per Article 35 GDPR, controllers are required to conduct **data protection impact assessments** (DPIAs) and, where necessary, to engage in **prior consultation** with the Italian Supervisory Authority under Article 36 GDPR. These procedures necessarily encompass an exhaustive appraisal of envisaged security measures, residual risks, and mitigation strategies.

It is further to be observed that, in Italy, **cybersecurity obligations imposed under parallel sectoral laws**—such as Legislative Decree No. 138 of 4 September 2024 (transposing Directive (EU) 2022/2555, "NIS2") and Regulation (EU) 2022/2554 ("DORA") for the financial sector—often intersect with personal data security duties, thereby necessitating an integrated compliance posture. Entities falling within the national cybersecurity perimeter or designated as "essential" or "important" under NIS2 are subject to additional layers of supervisory, technical, and incident response obligations, administered by the ACN and other competent sectoral authorities.

In sum, the personal data security obligations imposed within the Italian jurisdiction are not confined to abstract principles but are concretised through a panoply of substantive duties, procedural safeguards, and contextual benchmarks. These norms collectively require data controllers and processors to demonstrate, through documented evidence and continuous improvement, that their data protection governance systems are robust, proportionate, and responsive to both technological evolution and emerging threat landscapes.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The Italian legal framework, consistent with GDPR, imposes rigorous and multi-layered obligations upon

data controllers and processors in the event of a security breach implicating personal data—defined, in accordance with Article 4(12) GDPR, as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

This definitional construct is both technologically agnostic and substantively expansive, encompassing a broad array of incidents, whether occasioned by cyberattacks, human error, system failures, or unlawful access by internal or external actors.

Pursuant to Article 33 GDPR, the data controller is under a duty to notify the Italian Supervisory Authority without undue delay and, where feasible, no later than 72 hours after having become aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The obligation to notify must be accompanied by a breach report containing, at minimum, the nature of the breach, categories and approximate number of data subjects and records concerned, likely consequences, and the remedial measures taken or proposed. Where all such information cannot be provided concurrently, it may be submitted in phases, but must be fully documented to demonstrate accountability as required under Article 5(2) GDPR.

Where the data breach is likely to result in a high risk to the rights and freedoms of the individuals affected, Article 34 GDPR imposes a supplementary obligation to communicate the breach directly and without undue delay to the data subjects concerned. This communication must be clear and plain, and must describe in intelligible terms the nature of the breach, its potential consequences, and the measures undertaken to mitigate the impact. However, such communication may be exempted where (i) the controller has implemented appropriate technical and organisational protection measures that render the data unintelligible (e.g., encryption); (ii) subsequent measures have ensured that the high risk is no longer likely to materialise; or (iii) such communication would involve disproportionate effort, in which case public communication may be substituted.

In the Italian jurisdiction, the Garante has issued several interpretative acts and public FAQs specifying the contours of breach notification obligations, notably highlighting that failure to notify, or unjustified delay, may itself constitute a separate violation subject to sanctions under Article 83(4)(a) GDPR. Moreover, the obligation to notify applies not only to breaches occurring within the Union, but also to those occurring in third countries where the processing falls within the territorial or extraterritorial scope of Articles 3(1) and 3(2) GDPR.

Beyond regulatory notification, sector-specific regimes impose additional obligations. For example, providers of publicly available electronic communications services are subject to a parallel notification framework under Directive 2002/58/EC (as transposed by Article 32-bis of the Privacy Code), requiring them to notify both the Garante and, in some cases, subscribers and users of personal data breaches. Similarly, operators within the national cybersecurity perimeter, as designated under Legislative Decree No. 105 of 21 September 2019 and subsequent decrees under the purview of the Agenzia per la Cybersicurezza Nazionale (ACN), are required to report security incidents to CSIRT Italia and other competent sectoral authorities within designated timelines.

In practice, breach management in Italy requires the prior establishment of internal incident response protocols, breach detection mechanisms, and decision-making matrices that can be promptly activated upon breach detection. Controllers must also maintain a comprehensive breach register under Article 33(5) GDPR, documenting the facts surrounding the breach, its effects, and the remedial actions taken—irrespective of whether notification was ultimately required.

In conclusion, the Italian legal order, consonant with the GDPR architecture, subjects data controllers and processors to robust obligations in the event of personal data breaches, predicated upon risk-based triggers, strict notification timelines, and transparency requirements towards both authorities and affected individuals. The overarching regulatory ethos mandates readiness, speed, and proportionality, with the twin objectives of minimising harm and reinforcing systemic accountability.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, 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, and any exceptions.

Indeed, the Italian data protection framework, being fully harmonised with the provisions of GDPR, establishes an extensive and enforceable catalogue of rights for natural persons—designated as *data subjects*—which are aimed at safeguarding their informational self-determination, autonomy, and dignity. These rights are enshrined in Articles 12 through 23 GDPR and are directly applicable within the Italian legal system, further specified and, in limited circumstances, modulated by the Italian Privacy Code.

The principal rights accorded to data subjects include, but are not limited to:

(a) The Right of Access (Article 15 GDPR): Data subjects are entitled to obtain confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to such data along with information regarding the purposes of processing, categories of data concerned, recipients or categories of recipients, envisaged retention period, existence of rights to rectification or erasure, source of the data (if not collected from the data subject), and the existence of automated decision-making, including profiling. In Italy, this right is exercised through a request directed to the controller, who must respond within one month, extendable by two additional months in cases of complexity, with justification provided in writing.

(b) The Right to Rectification (Article 16 GDPR): Data subjects may request the correction of inaccurate personal data or the completion of incomplete data without undue delay. This right is of particular relevance in cases involving creditworthiness assessments, employment records, and health documentation.

(c) The Right to Erasure ("Right to be Forgotten," Article 17 GDPR): This right permits the data subject to obtain the erasure of personal data concerning them without undue delay in specific circumstances, including: where the data are no longer necessary in relation to the purposes for which they were collected; where consent is withdrawn and no other legal basis exists; where the data subject successfully objects to processing; where data have been unlawfully processed; or where erasure is required to comply with a legal obligation. In Italy, the *Garante* has clarified that erasure must also extend to third parties to whom the data have been disclosed, subject to the feasibility and proportionality of such communication.

(d) The Right to Restriction of Processing (Article 18 GDPR): This right allows data subjects to require the controller to limit the processing of their data under certain conditions—for instance, where accuracy is contested, where processing is unlawful but erasure is opposed, or where the controller no longer needs the data but the data subject requires it for legal claims. During restriction, data may only be stored and not processed otherwise, save for legal exceptions.

(e) The Right to Data Portability (Article 20 GDPR): Data subjects have the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format, and to transmit those data to another controller, where the processing is based on consent or contract and carried out by automated means. This right facilitates competition and data subject agency, particularly in financial, telecommunications, and health sectors.

(f) The Right to Object (Article 21 GDPR): Data subjects may object at any time, on grounds relating to their particular situation, to processing of their data based on public interest or legitimate interest, including profiling. The controller must cease processing unless it demonstrates compelling legitimate grounds. An absolute right to object applies where data are processed for direct marketing purposes.

(g) Rights in Relation to Automated Decision-Making and Profiling (Article 22 GDPR): Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless such processing is based on consent, contract, or authorised by law with suitable safeguards.

(h) The Right to Withdraw Consent (Article 7(3) GDPR): Where processing is based on consent, data subjects may withdraw such consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

These rights are exercised by submitting a request to the data controller, who is obliged under Article 12 GDPR to respond in a concise, transparent, intelligible, and easily accessible form. The controller must facilitate the exercise of data subject rights free of charge, except where requests are manifestly unfounded or excessive, in which case a reasonable fee may be charged or the request refused, with burden of proof resting on the controller.

Exceptions and limitations to these rights are narrowly construed and must be provided by Union or Member State law pursuant to Article 23 GDPR. In the Italian context, such limitations are codified in Articles 2-undecies and 2-duodecies of the *Italian Privacy Code* and may include processing carried out for reasons of national security, public order, prevention and prosecution of crimes, judicial independence, or rights and freedoms of others. For example, data subjects cannot access or request erasure of data processed by judicial authorities in the course of criminal investigations, or by the Anti-Mafia Registry where legal prohibitions apply.

Additionally, special rules govern the exercise of these rights in contexts involving minors, incapacitated persons, or deceased individuals (the latter regulated

under Article 2-terdecies *Italian Privacy Code*), where legal representatives, heirs, or appointees may act on behalf of the data subject.

In sum, the rights afforded to individuals under Italian data protection law are robust, comprehensive, and enforceable, reflecting a fundamental rights-based conception of data protection as anchored in Article 8 of the Charter of Fundamental Rights of the European Union and Article 2 of the Italian Constitution. Their exercise constitutes not merely a procedural prerogative but a substantive guarantee of individual sovereignty over personal information.

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

Within the Italian legal system, the right of individuals to initiate private civil actions for infringements of data protection rights is expressly recognised and operationalised in harmony with the provisions of GDPR and the Italian Privacy Code. The legal basis for such private right of action is found primarily in Article 82 GDPR, complemented by Articles 140-bis et seq. of the Italian Privacy Code and the broader principles of tortious liability codified in the Italian Civil Code (Articles 2043 and 2050).

Article 82 GDPR confers upon any person who has suffered material or non-material damage as a result of an infringement of the Regulation the right to receive compensation from the controller or processor responsible for the damage. This right is enforceable before national courts and is independent of any administrative sanctioning procedures that may be undertaken by the Italian Supervisory Authority.

Under Italian jurisprudence, the existence of a private right of action entails three cumulative conditions: (i) a proven violation of GDPR or national data protection provisions; (ii) the occurrence of damage, whether of a material or immaterial nature (such as reputational harm, distress, or anxiety); and (iii) a causal nexus between the unlawful processing and the alleged damage. The burden of proof concerning the occurrence and quantification of the damage rests with the claimant, while the controller or processor may only exonerate itself by demonstrating that it is in no way responsible for the event giving rise to the damage.

The national courts have progressively acknowledged the right to seek compensation for immaterial damages under Article 82 GDPR, even in the absence of economic loss, provided that the infringement results in concrete adverse effects on the data subject's dignity, privacy, or psychological well-being. Italian case law has confirmed that such damages are not presumed and must be established through evidence capable of substantiating the alleged harm.

In addition to individual claims, the Italian Privacy Code, through Article 140-bis, enables representative actions by associations and bodies that have been duly registered and recognised for the protection of fundamental rights and freedoms in the digital environment. These entities are entitled to act on behalf of data subjects to seek judicial redress, including compensation, declaratory relief, and injunctive measures, particularly in cases involving systemic or large-scale violations.

The procedural avenue for asserting such claims lies within the ordinary civil courts, under the rubric of "responsabilità extracontrattuale" (non-contractual liability), often accompanied by requests for interim or injunctive relief under Article 700 of the Italian Code of Civil Procedure. The coordination between administrative procedures before the Garante and private civil actions is governed by the principle of functional autonomy: the exercise of one does not preclude the other, although findings by the Garante may carry evidentiary weight in civil proceedings.

The Italian legal order thus ensures a robust and enforceable private right of action, both individually and collectively, for breaches of data protection rights, thereby reinforcing the accountability regime envisaged by the GDPR and ensuring that data subjects have recourse to effective remedies and judicial protection, in conformity with Article 79 GDPR and Article 47 of the Charter of Fundamental Rights of the European Union.

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

Under the Italian legal system, as harmonised with the GDPR, individuals whose personal data have been processed unlawfully or in breach of data protection obligations are unequivocally entitled to seek and obtain monetary compensation for the damage suffered, encompassing both material and non-material harms. This principle, established under Article 82 GDPR, is

directly applicable within the Italian jurisdiction and further supported by Article 15 of the Italian Privacy Code.

Article 82(1) GDPR expressly stipulates that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered". The liability regime under the GDPR is objectively constructed, with Article 82(3) imposing upon the controller or processor the burden of demonstrating that it is not in any way responsible for the event giving rise to the damage in order to escape liability.

The Italian courts have progressively embraced a broad and protective interpretation of the notion of "damage" (*danno*), aligning themselves with the expansive teleology of the GDPR and the jurisprudence of the Court of Justice of the European Union (CJEU). Notably, the recognition of non-material damage (*danno non patrimoniale*)—including reputational harm, emotional distress, anxiety, humiliation, and other injuries to dignity and personality rights—does not require the demonstration of economic or quantifiable loss. The Italian Corte di Cassazione has long held that the violation of fundamental rights enshrined in Articles 2 and 21 of the Italian Constitution, including the right to privacy and to the protection of personal identity, may per se give rise to compensable harm when the infringement is serious, non-trivial, and causally linked to the unlawful processing.

Recent Italian case law has affirmed the compensability of non-material damage arising from erroneous data registration in credit databases, unauthorised dissemination of personal data, excessive data retention, and failure to respond adequately to data subject requests under Articles 15 to 22 GDPR. In such cases, courts have awarded monetary damages for distress and reputational prejudice even in the absence of direct economic harm, provided that the claimant has demonstrated a concrete, personal, and immediate repercussion of the breach on his or her private sphere.

It is, however, necessary to emphasise that compensation is not automatic. The claimant must adduce evidence not merely of the unlawful conduct, but of the causal nexus (*nesso causale*) between the breach and the damage alleged. Italian civil procedural law, while permitting the presumption of certain psychological or moral injuries based on the nature of the infringement, still requires that the harm be plausible, non-fictitious, and substantiated by the factual matrix of the case.

Moreover, Article 82 GDPR does not require that the damage be "serious" in the sense of a de minimis threshold; the CJEU, in *UI v Österreichische Post AG* (Case C-300/21), has clarified that the mere existence of non-material damage is sufficient to trigger the right to compensation, even if such damage is minor, provided it is real and not hypothetical.

It is also noteworthy that under Article 140-bis of the Privacy Code, data subjects may avail themselves of collective redress mechanisms—class actions and representative claims—where multiple individuals are affected by systemic or large-scale data protection violations. These actions may be brought before the ordinary civil courts or, in certain cases, before the Garante, and may result in compensatory and injunctive relief.

In conclusion, Italian law, in harmony with the GDPR, grants individuals a robust right to compensation for both material and non-material damages resulting from breaches of data protection obligations. Such compensability is not contingent upon pecuniary loss, and encompasses a broad spectrum of psychological, reputational, and dignitary harms, provided that the infringement is adequately proven and causally linked to the detriment suffered.

30. How are data protection laws in your jurisdiction typically enforced?

The enforcement of data protection laws within the Italian jurisdiction is characterised by a dual structure of **administrative supervision** and **judicial adjudication**, with the Italian Supervisory Authority acting as the principal supervisory authority pursuant to Articles 51–59 of GDPR and Articles 144–160 of the Italian Privacy Code.

The Italian Supervisory Authority is endowed with comprehensive powers delineated under Article 58 GDPR, encompassing **investigatory**, **corrective**, **advisory**, and **authorisation** functions. Its enforcement activities are initiated either *ex officio*, pursuant to risk-based prioritisation or thematic inquiries, or *ex parte*, following data subject complaints or notifications of personal data breaches under Article 33 GDPR. The Authority's investigative tools include on-site inspections, document acquisition, interviews, technical audits, and cooperation with other competent authorities at both national and EU levels, including the EPDB and sectoral regulators such as the *Autorità Garante della Concorrenza e del Mercato* (AGCM) or the *Agenzia per la Cybersicurezza Nazionale* (ACN).

Upon identifying a breach of data protection law, the

Italian Supervisory Authority may adopt a variety of **corrective measures** under Article 58(2) GDPR, including warnings, reprimands, orders to comply, orders to communicate data breaches to data subjects, temporary or definitive limitations on processing, and the imposition of **administrative fines** under Article 83 GDPR. These fines are tiered: up to €10 million or 2% of global annual turnover for infringements of obligations under Articles 8, 11, 25–39 and 42–43 GDPR; and up to €20 million or 4% for violations of the basic principles of processing, data subject rights, or cross-border data transfers.

In Italy, such sanctions are imposed by formal **injunction orders** (*provvedimenti ingiuntivi*), which are subject to **judicial review** before the ordinary civil courts, typically the Tribunale Civile in Rome, in proceedings governed by Article 152 of the *Italian Privacy Code* and the *Codice di Procedura Civile*. Appeals may be lodged by either the sanctioned party or the data subject and may concern the legality, proportionality, or merits of the administrative act. Judicial oversight includes both procedural and substantive scrutiny and has, in several landmark rulings, resulted in the annulment, modification, or confirmation of Italian Supervisory Authority decisions.

In addition to administrative sanctions, certain data protection violations may give rise to **civil liability** under Article 82 GDPR, which grants data subjects the right to obtain compensation for material or non-material damage suffered as a result of unlawful processing. Such claims are adjudicated by the civil courts and are subject to ordinary rules of tort liability, evidentiary burden, and damages assessment, with jurisprudence recognising compensation for psychological distress, reputational harm, and loss of control over personal data.

In more serious cases, infringements may also entail **criminal liability** under Articles 167 to 170-bis of the *Italian Privacy Code*, which penalise unlawful data processing, aggravated disclosure or acquisition of personal data, and non-compliance with the *Garante*'s orders. Prosecution is initiated by the Public Prosecutor's Office, and penalties may include imprisonment and fines, particularly where the offence is committed with the intention of profit or involves sensitive categories of data.

Furthermore, the enforcement framework incorporates a strong component of **cooperative compliance and guidance**, with the Italian Supervisory Authority issuing general resolutions, best practice guidelines, codes of conduct, and FAQs aimed at fostering a culture of compliance. Controllers and processors are expected to proactively engage with the Authority through consultations under Article 36 GDPR, notifications of high-risk processing activities, or voluntary adherence to certification schemes and sectoral codes pursuant to Articles 40–43 GDPR.

It is also significant that Italy participates fully in the **one-stop-shop mechanism** and the **consistency mechanism** under Chapter VII GDPR, whereby cross-border cases involving multinational entities are coordinated through the EDPB, and lead supervisory authorities may propose binding decisions subject to peer review. The Italian Supervisory Authority has played an active role in such procedures, contributing to major pan-European enforcement actions, particularly in the digital platforms, cloud services, and behavioural advertising sectors.

In summary, data protection laws in Italy are enforced through a **multilayered system of administrative control, judicial protection, and criminal deterrence**, with the Italian Supervisory Authority exercising a pivotal role as both regulator and enforcer. The enforcement landscape is marked by increasing rigour, procedural sophistication, and international cooperation, reflecting the elevation of data protection from a sectoral regulatory concern to a matter of constitutional and fundamental rights.

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

The sanctionatory apparatus established within the Italian legal system for infringements of data protection laws mirrors the graduated and proportionate enforcement regime instituted by GDPR, which, being directly applicable, constitutes the cornerstone of punitive measures across the European Union. The Italian Privacy Code further delineates the modalities of application of such sanctions, including procedural safeguards, ancillary measures, and sector-specific adaptations.

Pursuant to Article 83 GDPR, the Italian Supervisory Authority is empowered to impose administrative fines of up to €10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements of provisions listed in Article 83(4). These include breaches relating to obligations of controllers and processors, obligations of certification bodies, and monitoring bodies under Articles 8, 11, 25 to 39, 42, and 43 GDPR.

For more severe infringements—falling under Article 83(5) GDPR—the administrative fines may reach up to €20 million or 4% of the total worldwide annual turnover. This category encompasses violations of the basic principles

for processing (including conditions for consent), data subjects' rights, international data transfers, and non-compliance with orders or limitations imposed by a supervisory authority.

Article 83(6) further empowers Member States to establish penalties, including criminal sanctions, for infringements not expressly covered by Articles 83(4) and (5), or in addition to administrative fines. In this context, the Italian Privacy Code, particularly under Articles 166 to 172-bis, provides for a complementary system of sanctions, both administrative and penal in nature.

Specifically, the Italian Supervisory Authority may impose additional corrective measures under Article 58 GDPR, such as warnings, reprimands, orders to bring processing into compliance, impositions of temporary or definitive limitations including bans on processing, and orders for rectification or erasure of personal data. These measures may be adopted autonomously or in conjunction with pecuniary sanctions.

Italian national law provides for penal sanctions in particular scenarios, such as the unlawful communication or dissemination of personal data subject to specific restrictions (Article 167 Italian Privacy Code), which may be punishable with imprisonment ranging from six months to three years. In cases of processing of special categories of personal data or data concerning criminal convictions and offences in violation of legal provisions, criminal penalties may also be triggered. The unlawful acquisition of personal data through fraudulent means is subject to imprisonment of up to four years.

The Italian Supervisory Authority, in determining the amount of the fine, exercises its discretion based on the criteria set forth in Article 83(2) GDPR, including the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage, the degree of responsibility of the controller or processor, previous infringements, cooperation with the supervisory authority, and any other aggravating or mitigating factor.

It is also noteworthy that, in line with the GDPR's accountability and transparency paradigm, sanctions imposed by the Italian Supervisory Authority are typically made public and, in cases of particular public interest or significant gravity, may be disseminated via press releases and listed on the official registry of measures. Such publication may entail reputational consequences and constitute an implicit additional deterrent effect.

In conclusion, the Italian jurisdiction ensures a comprehensive, graduated, and dissuasive system of sanctions for violations of data protection laws, rooted in the GDPR's enforcement provisions and integrated by national penal and administrative norms, thereby upholding the effectiveness and credibility of the data protection regime through both corrective and punitive instruments.

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

Within the Italian jurisdiction, the imposition and quantification of administrative fines for violations of data protection law is governed by the architecture of GDPR, notably Articles 83(1) to 83(7), as directly applicable, and further elucidated through interpretative practice by the Italian Supervisory Authority and the EPDB, particularly via the *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, adopted on 24 May 2023.

Article 83 GDPR establishes a bifurcated regime of sanctions: for certain breaches, the maximum fine may reach up to €10 million or 2% of the total worldwide annual turnover (whichever is higher); for others—typically those involving violations of core data protection principles, data subject rights, or conditions for consent—the ceiling rises to €20 million or 4% of the global annual turnover. These thresholds operate as absolute maximums and not as predetermined sanctions; the actual fine is to be determined on a case-by-case basis.

In Italy, the Italian Supervisory Authority is empowered, pursuant to Article 144 of the Privacy Code and Articles 58(2)(i) and 83 GDPR, to impose such fines either ex officio or upon complaint, with the underlying rationale being deterrence, proportionality, and effectiveness. Although no statutory tariff or rigid formula exists, the Italian Supervisory Authority applies a structured and reasoned approach in the quantification of pecuniary penalties.

The criteria that must guide the assessment are enumerated in Article 83(2) GDPR, and include:

– The nature, gravity and duration of the infringement; – The intentional or negligent character of the infringement; – Any actions taken to mitigate the damage suffered by data subjects; – The degree of responsibility of the controller or processor, taking into account technical and organisational measures; – Any relevant previous infringements; – The degree of cooperation with the

supervisory authority; – The categories of personal data affected; – The manner in which the infringement became known; – The adherence to approved codes of conduct or certification mechanisms; – Any other aggravating or mitigating factors, such as financial benefit gained from the infringement.

The Garante has embraced a graduated and cumulative approach, whereby each of the above elements is weighed and translated into an aggravating or mitigating coefficient, which in turn modulates the base amount determined by the typology and seriousness of the breach.

In practice, the Garante's decisions have disclosed an internal methodology, sometimes inspired by the EDPB Guidelines, whereby a base amount is first calculated on the basis of the violation tier, to which multipliers are then applied in light of the above criteria. For instance, fines against large multinational technology companies have typically been modulated in relation to the scale of processing, the number of data subjects affected, the systemic nature of the breach, and the lack of cooperation or repeat violations.

It is also of relevance that under Article 144-bis of the Privacy Code, in cases involving entities subject to sectoral supervision (e.g., financial institutions, telecom providers), the Garante may act in coordination with the respective regulatory authorities, which may result in compound or parallel sanctions, especially where the data breach also contravenes sector-specific obligations (e.g., PSD2, NIS2, DORA).

Furthermore, Italian administrative law principles—derived from the Statuto del Contribuente and general principles of legality, proportionality and due process—require that the imposition of the fine be preceded by a full adversarial procedure, wherein the controller is granted the opportunity to submit counterarguments and demonstrate extenuating circumstances.

Finally, while fines are the most visible sanction, the Garante may also impose a combination of corrective measures under Article 58(2) GDPR, including warnings, reprimands, suspension of processing, or ordering the controller to bring processing into compliance, with or without an accompanying fine.

In conclusion, although Italian law does not prescribe mechanical or codified thresholds for the quantification of fines, the process is governed by a combination of binding GDPR principles, structured interpretative criteria, and administrative precedent. The overarching imperative is to ensure that the sanctions imposed are effective, proportionate, and dissuasive, having regard to both the intrinsic gravity of the infringement and the contextual behaviour of the infringer.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions adopted by the Italian Supervisory Authority are **subject to judicial appeal** within the Italian legal system, in accordance with both national procedural law and the principles enshrined in GDPR.

Pursuant to Article 152 of the Italian Privacy Code, any **data subject**, **controller**, **processor**, or **other interested party** who is aggrieved by a decision, order, injunction, or sanction of the Italian Supervisory Authority may challenge such measure before the **ordinary civil courts**, and specifically before the **Tribunale ordinario competente per territorio**, which holds functional competence to assess the lawfulness and proportionality of the contested measure.

Where the enforcement decision emanates from the **Rome-based central authority** (as is typically the case), jurisdiction is commonly vested in the **Tribunale Civile di Roma**. The appeal is governed by the **summary cognition procedure** (*rito sommario di cognizione*) provided under Articles 702-bis et seq. of the *Codice di Procedura Civile*, which allows for expedited judicial review while ensuring full adversarial guarantees.

The applicant may request **the annulment, modification, or suspension** of the contested act, and may adduce evidence, expert testimony, or legal arguments pertaining to the interpretation and application of the GDPR, the *Italian Privacy Code*, and the *Garante*'s own regulatory framework. The Italian Supervisory Authority participates in such proceedings as a **necessary party**, and its legal representation is undertaken by the State Attorney's Office (*Avvocatura dello Stato*).

Furthermore, the same appeal route is available where the *Garante* has **refused to act** on a complaint or has dismissed it on grounds deemed unlawful or unreasonable. In this case, the data subject may bring an action not only for annulment of the dismissal but also to obtain a declaratory judgment affirming the existence of a data protection infringement and the obligation to adopt corrective measures.

The **judgment of the first instance court** is appealable to the **Corte d'Appello**, and, subsequently, issues of legality

and constitutional compatibility may be brought before the **Corte di Cassazione**, particularly where the dispute involves questions of interpretation of European law, subsidiarity of national remedies, or procedural guarantees under the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

In parallel, **data subjects retain the right to lodge a complaint with the *Garante*** under Article 77 GDPR and Article 141 *Italian Privacy Code*, independently of or in conjunction with judicial proceedings. The choice between the **administrative route** (complaint to the Italian Supervisory Authority) and the **judicial route** (civil litigation) is **non-exclusive** and may be exercised autonomously, though once a decision is rendered by the Italian Supervisory Authority, recourse must shift to the judiciary for further review.

Moreover, in the context of **cross-border processing activities**, enforcement decisions falling within the scope of the **one-stop-shop mechanism** under Articles 60–65 GDPR are also subject to **internal appeal procedures** established under the GDPR, coordinated by the EPDB. In such cases, binding decisions issued pursuant to Article 65 are not directly appealable at national level but may be subject to **annulment proceedings before the General Court of the European Union**, under Article 263 TFEU, where standing and procedural conditions are satisfied.

In conclusion, the Italian jurisdiction ensures a **robust and multilayered appellate framework** for the judicial scrutiny of data protection enforcement measures, combining administrative accountability, adversarial review, and hierarchical recourse, all situated within a broader system of constitutional and supranational guarantees. Such framework ensures that decisions of the *Garante* are not insulated from contestation, but are subject to legal oversight, procedural redress, and, where warranted, substantive reversal.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

The current orientation of Italian enforcement activity in the realm of data protection reveals a progressively accentuated focus on the scrutiny of artificial intelligence systems, particularly those employing generative capacities and biometric functionalities, with the Italian Supervisory Authority having recently subjected foreign AI providers to restrictive measures and substantial financial penalties for unlawful processing, deficient transparency, and insufficient risk mitigation. This emerging trajectory intersects with a renewed institutional emphasis on the integrity and security of digital infrastructures, as demonstrated by the imposition of record-setting administrative fines against prominent utilities and financial actors for the negligent protection of extensive personal data repositories, thereby underscoring the regulator's intolerance toward systemic vulnerabilities and insufficient breach response mechanisms. Moreover, the Italian supervisory authority continues to assert its historically vigilant stance vis-à-vis marketing communications and consent dynamics, directing enforcement initiatives toward entities engaged in indiscriminate telemarketing or reliant on legacy databases devoid of current and specific authorisations, particularly in contexts implicating data brokers and call centre intermediaries. Simultaneously, considerable attention is directed to the domain of workplace surveillance, with particular insistence on the illegitimacy of concealed or disproportionate employee monitoring practices absent prior compliance with statutory procedural safeguards under Article 4 of the Workers' Statute and corresponding data protection provisions. Finally, Italy's participation in the most recent G7 roundtable on data protection authorities reveals its strategic intent to position itself as a normative interlocutor in global regulatory dialogues, thereby consolidating an enforcement paradigm marked by cross-border alignment, policy harmonisation, and technological vigilance.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

Yes, the cybersecurity legislation in force within the Italian jurisdiction imposes a complex matrix of mandatory risk management measures and operational obligations upon both public and private entities, particularly those designated as operators of essential services, digital service providers, and entities included in the national cybersecurity perimeter. These obligations derive from a convergence of domestic and European sources, primarily Legislative Decree No. 138 of 4 September 2024 (transposing Directive (EU) 2022/2555, the “NIS2 Directive”), the Digital Operational Resilience Act (Regulation (EU) 2022/2554, “DORA”), and the Decreto-Legge No. 105 of 21 September 2019, as amended, which instituted the *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC).

Pursuant to Article 21 of the NIS2 Directive and its national transposition via D.Lgs. 138/2024, entities falling within the "essential" or "important" categories must adopt "appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which the entities use in the provision of their services". These measures must be informed by a risk-based approach and must ensure, at a minimum, the resilience, confidentiality, integrity, availability, and authenticity of the relevant systems and data.

The Implementing Regulation (EU) 2024/2690 further specifies the minimum technical and methodological requirements applicable to key categories of entities—such as DNS providers, cloud service providers, data centres, CDNs, online platforms, and social networks—mandating them to adopt controls aligned with international standards such as ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319 401, and CEN/TS 18026:2024. These include, *inter alia*, the definition of security policies, network segmentation, access controls, cryptographic safeguards, vulnerability management, secure configurations, supply chain security, and monitoring of incidents.

Complementarily, for financial institutions and ICT third-party service providers, DORA (Regulation (EU) 2022/2554), applicable directly since 17 January 2025, imposes a distinct layer of cybersecurity and operational resilience obligations. Articles 5 to 18 of DORA prescribe the development of a digital operational resilience strategy, governance structures involving the management body, incident detection and response procedures, and threat-led penetration testing (TLPT). Moreover, Articles 27 to 30 require the implementation of risk-based ICT third-party management policies, while Article 17 necessitates the continuous review and testing of ICT business continuity and disaster recovery plans.

At the national level, entities subject to the PSNC, designated via ministerial decrees and included in sectoral lists, are required—under D.L. 105/2019 and its attuative DPCMs—to implement a set of cybersecurity measures specified in the "Modello Nazionale per l'Implementazione delle Misure di Sicurezza" (v.1.0.1), published by the Agenzia per la Cybersicurezza Nazionale (ACN). These measures are categorised across five functional domains (Identify, Protect, Detect, Respond, Recover), in alignment with the NIST Cybersecurity Framework, and include asset inventory, network zoning, identity and access management, endpoint protection, incident handling procedures, and periodic vulnerability assessments.

Furthermore, organisations within the PSNC must appoint a *responsabile per la cybersecurity* (RCS), maintain a register of ICT assets, conduct regular security audits, and notify the CSIRT Italia and ACN of any incident potentially impacting ICT assets designated as critical. Failure to comply may result in administrative sanctions, suspension orders, or exclusion from public procurement procedures.

The Italian legal framework also intersects with sectoral regulations (e.g., AgID for public administrations, Bank of Italy circulars for financial operators, AGCOM for telecommunications), each of which may impose additional and sector-specific cybersecurity compliance duties.

In conclusion, Italian cybersecurity law—substantially expanded and systematised by the transposition of NIS2 and the entry into force of DORA—establishes a binding, risk-based obligation upon covered entities to implement specific, auditable and continuously updated cybersecurity risk management measures. These obligations are reinforced by supervision, reporting duties, and escalating sanctions, thus embedding cybersecurity not merely as a best practice but as a legal and strategic imperative across sectors of public interest and systemic relevance.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

Yes, the cybersecurity laws in force within the Italian legal order impose **stringent and increasingly codified obligations regarding supply chain cybersecurity management**, especially in light of the transposition of Directive (EU) 2022/2555 ("NIS2 Directive") via **Legislative Decree No. 138 of 4 September 2024**, and the direct applicability of **Regulation (EU) 2022/2554** ("Digital Operational Resilience Act" or "DORA") for financial sector entities. These instruments collectively define a normative framework in which **supply chain integrity and third-party risk management** constitute essential components of cybersecurity governance and compliance.

Under **Article 21(2)(d)** of Legislative Decree No. 138/2024, which implements Article 21(2)(d) NIS2, both **essential** and **important entities** are expressly required to adopt **appropriate and proportionate technical, operational and organisational measures** to manage risks originating from their **supply chains and supplier relationships**. These measures must extend to suppliers

of ICT services, products and systems upon which the continuity and security of critical or important services depend.

In this regard, entities must:

– identify critical dependencies within their supply chains; – assess cybersecurity risks associated with third-party providers; – incorporate **cybersecurity clauses** into contractual agreements; – monitor compliance with security obligations by suppliers on a continuous basis; – and ensure the integration of third-party security into their own risk management systems.

The **Agenzia per la Cybersicurezza Nazionale (ACN)**, in its capacity as national competent authority, may issue binding sector-specific or horizontal technical guidelines that further specify due diligence obligations, certification schemes, and compliance verification mechanisms applicable to third-party providers. Moreover, under **Article 23 of Decree No. 138/2024**, entities are required to notify the ACN not only of incidents affecting their own systems but also of **supply chain vulnerabilities or disruptions** that could materially impair the provision of essential services.

In the financial domain, **DORA** imposes a particularly robust and prescriptive framework for **ICT third-party risk management**. Under **Articles 28–30 of Regulation (EU) 2022/2554**, financial entities must maintain a comprehensive register of information on all ICT third-party service providers, carry out pre-contractual due diligence, and continuously monitor performance, resilience, and compliance with security requirements. For providers supporting **critical or important functions**, entities must ensure that contracts include provisions on:

– service availability, integrity and confidentiality; – access, audit, and termination rights; – data localisation, encryption, and incident notification obligations; – and compliance with Union and national regulations.

Additionally, DORA foresees the designation of **Critical ICT Third-Party Service Providers (CTPPs)** by the European Supervisory Authorities (ESAs), who shall be subject to **direct oversight at EU level**, but whose security posture will impact the compliance obligations of Italian financial entities operating within their purview. In this light, financial entities must reassess their **outsourcing and vendor governance strategies**, aligning them with the resilience benchmarks and monitoring protocols introduced by **Delegated Regulation (EU) 2024/1773**, which operationalises DORA's requirements for ICT third-party risk management.

Within the perimeter of **national cybersecurity**, further obligations arise for public administrations and operators of critical infrastructure designated under **Decree-Law No. 105 of 21 September 2019**, converted by Law No. 133 of 18 November 2019. These subjects must submit for ACN approval a **list of ICT components and services** acquired through the supply chain and may be prohibited from using non-vetted suppliers, particularly when national security or strategic sovereignty is implicated. The *Modello Nazionale delle Misure Minime di Sicurezza* further requires the inclusion of **supplier security assessments**, vetting protocols, and contractual enforcement mechanisms in organisational cybersecurity policies.

Moreover, certain **sectoral regulations**—such as in telecommunications (Legislative Decree No. 259/2003), health, and transport—include specific procurement and accreditation rules regarding the security of outsourced ICT systems, medical devices, and automation technologies, often linked to certification under schemes developed pursuant to **Regulation (EU) 2019/881** ("Cybersecurity Act").

In conclusion, the Italian cybersecurity legal framework—mirroring and operationalising EU law—imposes **concrete, risk-based, and enforceable supply chain security obligations**, whose scope extends well beyond passive awareness to include active contractual management, continuous oversight, and integration into broader cyber risk governance systems. Non-compliance exposes entities to administrative sanctions, reputational damage, and, in cases involving public interest sectors, potential exclusion from public procurement or critical service provision.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

Yes, the cybersecurity legislation currently in force within the Italian jurisdiction imposes a multiplicity of obligations relating to the transmission, notification, and structured sharing of information, both toward public authorities and, in certain cases, within sectoral or inter-organisational frameworks, pursuant to normative sources of national and supranational provenance. The cornerstone of this regime is constituted by Legislative Decree no. 138 of 4 September 2024, which transposes Directive (EU) 2022/2555 (so-called "NIS2 Directive"), and which imposes upon "essential" and "important" entities rigorous duties of notification, cooperation, and disclosure vis-à-vis the Agenzia per la Cybersicurezza Nazionale (hereinafter, "ACN"), designated therein as the

National Competent Authority.

Pursuant to Article 23 of Directive (EU) 2022/2555, as transposed in Italy, organisations are subject to a tiered incident notification obligation, mandating the initial notification of any significant incident—defined as one having a substantial impact on the provision of services—within 24 hours of becoming aware thereof, followed by a formal incident notification within 72 hours and a conclusive report to be transmitted within one month. Such notifications must include all information necessary to enable the ACN and the Computer Security Incident Response Team Italia (CSIRT) to assess the impact, mitigate propagation effects, and initiate coordinated response activities. A parallel obligation exists in respect of cyber threats "with the potential to result in a significant incident," in line with a proactive approach to threat intelligence and situational awareness.

The Italian cybersecurity legal order also provides for information-sharing requirements under the "Perimetro di Sicurezza Nazionale Cibernetica," established by Decree-Law no. 105 of 21 September 2019 and further developed through DPCM nos. 81 and 131 of 2020. Entities falling within the Perimetro are subject to a regulatory framework that mandates the transmission to the ACN of (i) an updated inventory of critical ICT assets, (ii) reports concerning vulnerabilities or anomalies affecting such assets, and (iii) periodic security posture reports as prescribed in the "Modello delle Misure Minime." These provisions operate in conjunction with specific obligations of notification relating to the implementation of security measures and the occurrence of incidents affecting ICT assets deemed strategic for national security.

Additional obligations arise under sector-specific cybersecurity regimes, such as those applicable to financial entities under Regulation (EU) 2022/2554 (Digital Operational Resilience Act, "DORA"), which entered into force in January 2023 and is fully applicable from January 2025. DORA imposes upon financial institutions, insurance undertakings, and critical ICT third-party service providers a duty to report major ICT-related incidents and significant cyber threats to the relevant national competent authorities, including the Bank of Italy and CONSOB, in accordance with delegated acts such as Commission Delegated Regulation (EU) 2024/1773, which specifies the content and format of contractual arrangements and notification requirements vis-à-vis third-party service providers.

In parallel, under Article 40 of Legislative Decree no. 138/2024 and the Determination of the Director General of the ACN no. 38565 of 26 November 2024, all NIS entities are required to register on the ACN's digital platform and provide detailed information regarding their cybersecurity governance, supply chains, and technical contacts for incident response, thereby facilitating continuous exchange of security-relevant information. Furthermore, such entities must designate one or more representatives within the European Union for purposes of cross-border coordination and information exchange, thereby aligning domestic provisions with the interoperability requirements of the NIS2 cooperation group and the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe).

In conclusion, the Italian cybersecurity framework imposes a multifaceted and interinstitutional regime of information sharing, oriented toward preventive risk mitigation, coordinated incident management, and the construction of a distributed national cyber-resilience capacity, wherein regulated entities are obliged to act not only as individual custodians of their own ICT security but as integrated nodes within a broader national and European cybersecurity architecture.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

Yes, the cybersecurity regulatory framework applicable within the Italian jurisdiction mandates, for certain categories of public and private entities, the formal appointment of dedicated individuals bearing specific responsibilities in the domain of cybersecurity, including but not limited to the roles of *Responsabile per la Cybersecurity*, Chief Information Security Officer (CISO), and regulatory points of contact with institutional authorities. These requirements emanate primarily from Legislative Decree No. 138 of 4 September 2024 (implementing Directive (EU) 2022/2555, the "NIS2 Directive"), the national *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC) instituted by D.L. No. 105 of 21 September 2019, and its implementing decrees, notably the DPCM No. 131/2020 and the ACN's Determination No. 38565/2024.

Under Article 5 of the aforementioned D.L. 105/2019 and the provisions of the DPCM 131/2020, all entities included in the PSNC are required to formally designate a cybersecurity officer (*Incaricato per la Cybersecurity*) and a technical representative (*Referente Tecnico per la Cybersecurity*) responsible for implementing and

supervising compliance with the technical and procedural security measures mandated by the ACN through the national implementation model.

Specifically, the *Incaricato*:

– Acts as the hierarchical referent for all organisational activities related to the enforcement of cybersecurity obligations under the PSNC; – Ensures the implementation and verification of minimum security measures, including asset inventory, risk management, access controls, and network segmentation; – Supervises the proper notification of incidents as required by Article 1(3)(a) of D.L. 105/2019; – Liaises directly with the ACN and contributes to national cybersecurity crisis management frameworks under Article 5 of the same decree; – Coordinates internal audits and facilitates external inspections conducted by ACN-appointed entities.

Concomitantly, the *Referente Tecnico*:

– Serves as the primary operational contact for CSIRT Italia for the purpose of incident handling and threat intelligence; – Provides technical support to the *Incaricato* and ensures compliance with hardening, patching, vulnerability assessment, and monitoring obligations; – Maintains updated logs of the organisation's network topologies, software platforms, and communication flows; – Coordinates with the organisation's IT department and, where appointed, the DPO, to ensure integrated risk management.

Their identification and contact details must be formally communicated to the ACN, which in turn shares such information with the Presidency of the Council of Ministers and sectoral authorities for coordination and oversight purposes, pursuant to the ACN Determination No. 38565/2024.

Moreover, under the DORA Regulation (EU) 2022/2554, applicable from January 2025 to financial entities, the management body of each entity is legally responsible for the approval, implementation, and periodic review of the digital operational resilience strategy. Although the regulation does not impose the use of a specific title (such as CISO), it de facto requires the appointment of a person or structure vested with operational responsibility for the internal governance of ICT risk, including incident classification, risk assessments, testing, and third-party oversight.

Likewise, Legislative Decree No. 138/2024 (NIS2 transposition) mandates, under Article 5 and Article 21, the adoption of governance structures capable of overseeing and executing cybersecurity policies, and requires entities to ensure that appropriate human resources are designated for interface with competent authorities, including for incident notification (Articles 23–24). In practice, this entails the designation of one or more natural persons who assume the functional prerogatives of a CISO, even where such title is not explicitly used.

Failure to appoint the required cybersecurity figures, or to ensure their qualification and operational independence, may constitute a breach of the relevant obligations, resulting in the imposition of corrective measures or financial penalties by the ACN (in the case of PSNC or NIS2 entities) or by other competent supervisory authorities (e.g., Bank of Italy, CONSOB).

In conclusion, the Italian legal system requires, for strategically and infrastructurally significant entities, the formal and traceable appointment of cybersecurity officers with well-defined technical and regulatory duties. These individuals represent the fulcrum of institutional interaction, risk governance, and internal accountability, forming an indispensable element of the national and European cybersecurity architecture.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

Yes, the Italian legal system, while adhering to a unified framework of cybersecurity governance at the national level—principally through the implementation of Directive (EU) 2022/2555 ("NIS2") and Regulation (EU) 2022/2554 ("DORA")—also establishes **industry-specific cybersecurity obligations** across various sectors of critical relevance, such as **finance, healthcare, telecommunications, energy, transportation, and public administration**. These obligations are grounded both in **EU harmonised legislation** and **sectoral laws and regulations** adopted at the domestic level, often with the involvement of distinct supervisory authorities.

1. Financial Sector – DORA and Complementary National Measures

In the financial domain, the entry into force of the **Digital Operational Resilience Act (Regulation (EU) 2022/2554)** on 17 January 2025 introduced a comprehensive, horizontally applicable regulatory regime mandating financial entities—including banks, insurers, investment firms, payment service providers, and crypto-asset service providers—to implement **robust ICT risk**

management frameworks, **resilience testing programmes**, and **third-party risk oversight mechanisms**.

Entities are required to: – perform risk-based ICT assessments; – conduct advanced testing (e.g., threat-led penetration testing, TLPT); – report ICT-related incidents to competent authorities, including the Bank of Italy and CONSOB; – and ensure contractual compliance and security assurance from ICT third-party service providers.

DORA is supplemented by **Delegated Regulations (EU) 2024/1773 and 2024/1774**, which specify technical standards for ICT third-party risk management and simplified frameworks for less complex entities. Enforcement lies with sector-specific national regulators, acting in coordination with European Supervisory Authorities (ESAs) and the **Agenzia per la Cybersicurezza Nazionale (ACN)**.

2. Healthcare Sector – eHealth and Cybersecurity Obligations

Healthcare entities are subject to heightened cybersecurity obligations under both NIS2 and **sector-specific regulations**. Pursuant to **Article 3 of Legislative Decree No. 138/2024**, hospitals, regional health authorities, pharmaceutical operators, and electronic health record platforms may qualify as **essential or important entities** under NIS2 and must:

– implement risk-based security measures for health data and critical medical infrastructure; – report cyber incidents and vulnerabilities to ACN; – adhere to organisational and technical standards issued by the Ministry of Health and ACN.

Moreover, **health data processing** is governed by stringent security rules under Article 9 GDPR and Article 2-septies *Italian Privacy Code*, with operational security measures to be derived from guidance issued by the Garante and based on **ISO/IEC 27001 and 27799 standards**.

3. Telecommunications – Legislative Decree No. 259/2003 (Codice delle Comunicazioni Elettroniche)

Operators of public electronic communications networks and services are bound by cybersecurity obligations codified in **Articles 16-bis et seq.** of the **Codice delle Comunicazioni Elettroniche**, as amended to align with NIS2. These include:

– implementation of appropriate security measures; – reporting of significant incidents to both **AGCOM** and **ACN**; – and participation in resilience enhancement programmes such as network redundancy and anti-DDoS systems.

AGCOM, as sectoral regulator, cooperates with ACN for compliance assessment and enforcement.

4. Energy Sector – Legislative Decree No. 93/2011 and ARERA Regulations

Energy operators, particularly those in the **electricity, gas, and oil sectors**, are designated as critical operators under NIS2 and are supervised by **ARERA (Autorità di Regolazione per Energia Reti e Ambiente)** in coordination with ACN. These entities must:

– comply with cyber resilience measures tailored to SCADA and ICS systems; – adopt secure-by-design principles for grid infrastructure; – and report cyber incidents affecting the continuity or reliability of supply.

ENISA's guidelines on the cybersecurity of smart grids and critical energy infrastructure inform national best practices.

5. Transport Sector – Legislative Decree No. 35/2011 and Ministry Regulations

Airports, railway operators, maritime authorities, and urban mobility platforms fall within NIS2 and are also subject to industry-specific cybersecurity regulations coordinated by the **Ministry of Infrastructure and Transport**, which defines sectoral risk management requirements, often aligned with **NIS Cooperation Group recommendations** and **ENISA sectoral guidance**.

6. Public Administration and Critical Infrastructure – National Cybersecurity Perimeter

Pursuant to **Decree-Law No. 105 of 21 September 2019**, converted by **Law No. 133 of 18 November 2019**, and further operationalised by **DPCM No. 131/2020**, public administrations and operators of national strategic interest are subject to the **National Cybersecurity Perimeter**. Entities within the perimeter must:

– register all ICT systems and components; – submit risk assessments and vulnerability reports; – undergo ACN-led security audits; – and notify all incidents within strict deadlines.

The perimeter encompasses sectors such as defence, aerospace, justice, finance, and telecommunications.

40. What impact do international cybersecurity standards have on local laws and regulations?

The impact of international cybersecurity standards on the Italian legal and regulatory landscape is both systemic and constitutive, functioning not merely as interpretative aids or best practice guidelines, but as integral instruments for the concretisation of legal obligations under both national and European Union law. The incorporation, reference, and sometimes the de facto adoption of such standards occur through legislative provisions, regulatory decrees, and authoritative guidance issued by national bodies such as the Agenzia per la Cybersicurezza Nazionale (ACN), the Italian Supervisory Authority, and sectoral regulators.

Foremost among these standards are the ISO/IEC frameworks—especially ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 27002 (security controls), ISO/IEC 22301 (business continuity), and ISO/IEC 27005 (risk management)—which are repeatedly referenced in both the *Perimetro di Sicurezza Nazionale Cibernetica* (D.L. 105/2019 and DPCM 131/2020) and the legislative corpus implementing Directive (EU) 2022/2555 (NIS2 Directive). Article 21 of the NIS2 Directive and its Italian transposition via Legislative Decree No. 138 of 4 September 2024 expressly mandate that security measures and risk management protocols be aligned with "relevant European and international standards", and this has been operationalised through the ACN's Determination No. 38565/2024 and subsequent implementing acts.

Furthermore, Regulation (EU) 2024/2690, which specifies the technical and methodological requirements under Article 21 NIS2, explicitly lists ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319 401, and CEN/TS 18026:2024 as foundational benchmarks for compliance. These standards are thus not optional or merely aspirational, but constitute the substantive matrix against which conformity is assessed by supervisory authorities, including the ACN and CSIRT Italia.

Similarly, the Digital Operational Resilience Act (DORA), applicable from January 2025 to the financial sector, embeds the application of international standards into its operational mandates, requiring financial entities to adopt testing, auditing, risk analysis, and third-party management strategies that are, in substance, indistinguishable from those codified in ISO/IEC and NIST standards.

Moreover, under the PSNC framework, entities are obligated to implement a set of minimum security measures published in the "Modello Nazionale per l'Implementazione delle Misure di Sicurezza" (v.1.0.1), which closely reflect the structure and content of NIST CSF and ISO/IEC 27001:2022, thereby incorporating them by reference. In particular, these standards inform the organisation's obligations concerning risk assessment, access control, incident response, data integrity, and supply chain security.

Additionally, the Italian judiciary and administrative bodies—including the Italian Supervisory Authority—frequently invoke international standards in their interpretative and sanctioning activities. The Garante's decisions regularly cite adherence or deviation from ISO 27001 and related standards as probative of whether the controller has fulfilled its obligations under Article 32 GDPR (security of processing) and Article 25 (data protection by design and by default).

In the context of certifications, Article 42 GDPR and its Italian corollary under Article 13 of the Privacy Code encourage the adoption of certification schemes based on international standards. Italian certification bodies, accredited by Accredia under ISO/IEC 17065, offer conformity assessments based on ISO/IEC 27701 (privacy information management) and ISO/IEC 27001.

The normative penetration of international standards is also evident in public procurement, where compliance with ISO/IEC standards is often a prerequisite in tender specifications, particularly where critical ICT systems are involved. Moreover, ENISA and the European Cybersecurity Certification Framework under Regulation (EU) 2019/881 ("Cybersecurity Act") reinforce the binding role of such standards in establishing the baseline criteria for EU-wide certification schemes.

In conclusion, international cybersecurity standards do not merely influence but fundamentally structure the content, scope, and interpretation of cybersecurity obligations under Italian law. Their normative function is hybrid: simultaneously substantive (defining legal duties), procedural (informing compliance methodologies), and evidentiary (establishing presumptions of diligence or negligence). As such, they form an indispensable axis of the Italian cybersecurity compliance and enforcement regime.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be

reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Yes, Italian cybersecurity legislation imposes a comprehensive suite of **obligations concerning the detection, management, and reporting of cybersecurity incidents**, which are defined, classified, and regulated within both **horizontal frameworks** (such as the GDPR and NIS2) and **sector-specific regimes** (including DORA, the National Cybersecurity Perimeter, and telecommunications law).

1. Definition of Cybersecurity Incident

Under **Legislative Decree No. 138 of 4 September 2024**, which transposes **Directive (EU) 2022/2555 (NIS2)**, a **cybersecurity incident** is defined in line with Article 6 NIS2 as:

"An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems."

This definition is further nuanced by implementing regulations and technical guidance from the **Agenzia per la Cybersicurezza Nazionale (ACN)**, which classifies incidents based on their impact, propagation potential, and criticality of the affected services.

2. Mandatory Notification Obligations – NIS2 Entities

Essential and important entities, as defined under Articles 3 and 6 of Legislative Decree No. 138/2024, are required to:

– **Notify the ACN** without undue delay and, in any event, within **24 hours** of becoming aware of a significant incident (Article 23); – Provide an **initial notification** outlining the nature of the incident, the suspected or known cause, and immediate mitigation measures; – Submit a **detailed follow-up report** within **72 hours**, including technical analysis, impact assessment, response actions, and any cross-border implications; – File a **final report** within **one month**, describing long-term mitigation strategies and residual vulnerabilities.

The ACN is authorised to disseminate anonymised incident data to relevant sectoral authorities, CERTs, or other NIS cooperation entities, and to require the entity to inform impacted third parties or clients when necessary to prevent further damage.

Entities must also notify any **newly discovered vulnerabilities** that could be exploited to compromise network and information systems.

3. Personal Data Breaches – GDPR

Pursuant to **Article 33 GDPR**, all data controllers must notify the **Garante per la Protezione dei Dati Personali** of a **personal data breach** within **72 hours**, where the breach is likely to result in a risk to the rights and freedoms of natural persons. The notification must include:

– a description of the nature of the breach; – categories and approximate number of data subjects and records affected; – contact details of the data protection officer (if any); – likely consequences; – and measures taken to address the breach.

Where the risk is **high**, **Article 34 GDPR** requires **communication to the affected individuals** without undue delay, unless effective technical safeguards (e.g., encryption) neutralise the risk, or if such notification would involve disproportionate effort—whereby public disclosure may suffice.

4. Financial Sector – DORA

Under **Regulation (EU) 2022/2554 (DORA)**, as of 17 January 2025, financial entities must report **major ICT-related incidents** to their competent financial supervisors (e.g., Bank of Italy, CONSOB). The notification timeline is even stricter than NIS2:

– **Initial notification** within **4 hours** of classification as a major incident; – **Intermediate updates** as the situation evolves; – **Final report** within **one month**, addressing root cause analysis, impacts, mitigation, and lessons learned.

Entities must also report incidents to affected clients if the incident has a material adverse impact on service delivery.

The scope includes cyberattacks, system failures, third-party disruptions, and data integrity breaches. Coordination with the ACN and the European Supervisory Authorities (ESAs) is also required, particularly in cross-border cases or those affecting Critical ICT Third-Party Providers (CTPPs).

5. Telecommunications Sector – Codice delle Comunicazioni Elettroniche

Pursuant to **Article 16-bis** of Legislative Decree No. 259/2003, operators of public electronic communications services must:

– Notify **AGCOM** and **ACN** of security breaches or significant service degradations; – Cooperate with **CERT-ACN** for technical remediation; – Inform users if the breach is likely to adversely affect their personal data or

service continuity.

6. National Cybersecurity Perimeter – Law No. 133/2019 and DPCM No. 131/2020

Operators designated within the **National Cybersecurity Perimeter** must:

– Notify the **ACN immediately** of any incident affecting ICT assets designated as critical; – Provide detailed incident documentation through the national cybersecurity platform (as regulated by Determinazione ACN No. 38565/2024); – Submit to audits and corrective plans imposed by the ACN.

Failure to notify or cooperate exposes the entity to administrative fines, suspension of activity, or exclusion from strategic supply chains.

7. Notification to Law Enforcement or Sectoral Authorities

Where incidents involve **criminal activity** (e.g., ransomware, data theft, system sabotage), notification to **law enforcement** (i.e., Postal Police or Public Prosecutor) is required or strongly recommended. In certain cases, the **ACN** may also transmit the information directly to judicial or investigative authorities pursuant to Article 7 of Law No. 109/2021.

42. How are cybersecurity laws in your jurisdiction typically enforced?

The enforcement of cybersecurity laws within the Italian jurisdiction is characterised by a multilevel and functionally differentiated architecture involving administrative, sectoral, and, where applicable, criminal law instruments, all coordinated through central regulatory bodies and sector-specific authorities. This system ensures both ex ante compliance and ex post accountability across the strategic, operational, and technical dimensions of cybersecurity governance.

The principal authorities vested with enforcement powers include:

1. Agenzia per la Cybersicurezza Nazionale (ACN): Instituted by D.L. No. 82/2021 and reinforced by Legislative Decree No. 138/2024 (transposing Directive (EU) 2022/2555 – NIS2 Directive), the ACN functions as the national competent authority for cybersecurity, the NIS single point of contact, and the designated oversight body for the *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC). The ACN exercises its enforcement prerogatives through:

– *Inspections and audits*, either periodically or in response to incidents or non-compliance notifications; – *Corrective orders*, including the imposition of specific technical and organisational measures; – *Administrative fines* and exclusion from procurement procedures, as foreseen by Article 28 of D.L. 105/2019; – *Coordination with CSIRT Italia*, which monitors, detects and manages cyber incidents and contributes intelligence to enforcement assessments.

2. Garante per la Protezione dei Dati Personali: With jurisdiction over cybersecurity incidents involving personal data (e.g., data breaches, unlawful processing, or inadequate security), the Garante enforces Articles 32–34 GDPR and the relevant provisions of the Privacy Code. Enforcement modalities include:

– *Investigative powers*, including on-site inspections, seizure of documentation, and forensic analysis; – *Sanctions*, including pecuniary fines under Article 83 GDPR, temporary or definitive processing bans, and public reprimands; – *Preliminary measures* (e.g., urgenti provvedimenti cautelari) in case of imminent harm; – *Publication of sanctioning decisions*, thereby exerting reputational deterrence.

3. Sectoral Regulators: Authorities such as the *Banca d'Italia*, *CONSOB*, *AGCOM*, and *ARERA* retain complementary enforcement powers over regulated sectors (e.g., finance, telecommunications, energy), where cybersecurity intersects with prudential or operational resilience. They may:

– Impose additional risk management obligations under sectoral legislation; – Conduct thematic inspections in collaboration with the ACN; – Issue binding recommendations or impose administrative penalties.

4. Judicial Enforcement and Criminal Liability: Although cybersecurity law is primarily administrative and preventive, criminal enforcement may arise in cases involving:

– *Unlawful access to computer systems* (Art. 615-ter Penal Code); – *Data destruction or deterioration* (Art. 635-bis); – *Interception of communications* (Art. 617-quater); – *Cyberterrorism or attacks against critical infrastructure*, which may trigger national security responses.

Public prosecutors may act autonomously or upon referral from regulatory bodies, particularly where incidents impact public safety, national defence, or vital services. The law also contemplates civil liability for

damages under Article 2043 of the Civil Code, GDPR Article 82, and the general rules on tort and contract.

5. Incident Notification and Response: Enforcement is often triggered by mandatory notifications. Entities under NIS2/PSNC must notify significant incidents to the CSIRT Italia and ACN within specified deadlines (e.g., within 24 hours for initial notification). DORA requires a similar structure for the financial sector, with ICT-related incident classification and reporting obligations to competent authorities. Non-notification or false notification is itself subject to sanction.

6. Supervisory Cooperation: Italian authorities collaborate with European bodies under the auspices of ENISA, the European Cyber Crises Liaison Organisation Network (EU-CyCLONe), and cross-border supervisory colleges (notably under DORA and GDPR). These cooperative frameworks enhance enforcement reach, harmonisation, and interoperability of sanctions.

In sum, cybersecurity laws in Italy are enforced through an integrated, multi-authority ecosystem that combines preventive regulation, reactive sanctioning, technical supervision, and, where necessary, judicial prosecution. Enforcement is predicated on a combination of risk-based assessments, sectoral criticality, and institutional coordination, and aims to ensure resilience, accountability, and strategic autonomy across the national cyber domain.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

In the Italian jurisdiction, regulators entrusted with the enforcement of cybersecurity laws are vested with **extensive powers of oversight, inspection, and audit**, structured around a **multi-authority supervisory architecture** that reflects both the stratified nature of national sectoral regulation and the supranational imperatives arising from the transposition of **Directive (EU) 2022/2555 (NIS2)** and the direct applicability of **Regulation (EU) 2022/2554 (DORA)**. The relevant authorities exercise such powers **autonomously and, where required, in coordination**, depending on the sector, criticality, and nature of the operator concerned.

1. Agenzia per la Cybersicurezza Nazionale (ACN) – National NIS Authority

As the designated **national competent authority under NIS2**, the **ACN** exercises **primary supervisory authority** over all **essential and important entities** falling within the scope of **Legislative Decree No. 138 of 4 September 2024**, as well as over operators designated under the **National Cybersecurity Perimeter** established by **Law No. 133/2019** and **DPCM No. 131/2020**.

The ACN's powers include:

– **Unrestricted access** to facilities, information systems, and documentation (Art. 28, D.Lgs. 138/2024); – The ability to **conduct on-site inspections**, with or without prior notice, including forensic collection, penetration testing, and configuration auditing; – The right to **summon personnel**, request written statements, and examine internal policies, logs, and supplier contracts; – Imposition of **remediation plans** (*piani di adeguamento*), timelines for compliance, and continuous monitoring; – Authority to conduct **sectoral or cross-sectoral audits**, independently or in coordination with other authorities (e.g., AGCOM, ARERA, Ministry of Health); – Competence to **suspend or restrict operations**, impose administrative sanctions, or refer violations for criminal prosecution.

The ACN also administers the **national cybersecurity platform** through which operators submit compliance documentation, incident reports, and supply chain declarations, as formalised in **Determination No. 38565/2024**.

2. Bank of Italy, CONSOB, IVASS – Financial Sector Oversight under DORA

Under **Regulation (EU) 2022/2554 (DORA)**, national financial regulators possess **direct supervisory powers** over banks, insurance undertakings, payment institutions, and investment firms. These powers include:

– **Full audit rights** over ICT risk management frameworks, business continuity policies, third-party contracts, and testing documentation (Art. 31 DORA); – Authority to **review incident registers**, enforce ICT-related governance obligations, and **verify data integrity and resilience**; – Capacity to conduct **on-site or remote inspections**, with recourse to technical experts or joint supervisory teams established under the European Supervisory Authorities; – Imposition of **administrative sanctions** and **corrective measures**, including mandatory risk remediation plans and prohibition on reliance upon non-compliant ICT third parties; – Referral to ACN or the European Oversight Forum for issues relating to **Critical ICT Third-Party Providers (CTPPs)**.

3. AGCOM and AGID – Telecommunications and Public Administration

The **Autorità per le Garanzie nelle Comunicazioni (AGCOM)**, in cooperation with the **Agenzia per l'Italia**

Digitale (AGID) and the **ACN**, supervises electronic communications service providers and public sector digital operators.

Their powers include:

– Oversight of **minimum security standards** under the *Codice delle Comunicazioni Elettroniche* (D.Lgs. 259/2003); – **Technical inspections** of network integrity, encryption policies, and incident response capabilities; – Enforcement of compliance with **certification requirements**, procurement restrictions, and incident reporting thresholds; – Right to **suspend digital public services** in cases of systemic vulnerability or persistent non-compliance.

4. Garante per la Protezione dei Dati Personali – Data Protection and Security Enforcement

While not a cybersecurity regulator *sensu stricto*, the **Garante** plays a decisive role in **cybersecurity oversight insofar as personal data security** is implicated, pursuant to **Articles 5(1)(f) and 32 GDPR** and Articles 33–36 for breach and DPIA obligations.

The Garante may:

– Conduct **dawn raids**, seize documentation, and access encrypted storage; – Order the **suspension or rectification of insecure processing activities**; – Impose **administrative fines** under Article 83 GDPR for inadequate security measures, failed breach notification, or non-cooperation; – Cooperate with the ACN or judicial authorities where breaches have national security or cross-sectoral ramifications.

5. Cross-Authority and EU-Level Cooperation

Supervisory authorities in Italy participate in coordinated inspection and enforcement through:

– **Joint supervisory teams** under the DORA framework; – **Cross-border inspection mechanisms** under NIS2 and the **NIS Cooperation Group**; – Joint enforcement actions with the EPDB, especially in data breach scenarios; – Referral of violations involving AI, biometric surveillance, or systemic infrastructure to competent sectoral regulators.

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

The Italian legal system, in transposing and operationalising the sanctions regime envisaged under Directive (EU) 2022/2555 (NIS2 Directive) through Legislative Decree no. 138 of 4 September 2024, has instituted a stratified system of administrative and, in certain instances, penal sanctions applicable to entities—whether classified as essential or important—falling within the perimeter of cybersecurity obligations. Such sanctions are imposed in a proportionate, dissuasive, and effective manner, in accordance with Article 34 of the aforementioned Directive, and are administered by the Agenzia per la Cybersicurezza Nazionale (ACN), which exercises oversight and enforcement functions as the designated National Competent Authority.

In quantitative terms, the Decree introduces administrative pecuniary sanctions that reach a ceiling of €10,000,000 or 2% of the total annual worldwide turnover of the offending undertaking for breaches committed by operators deemed "essential entities." For "important entities," the ceiling is fixed at €7,000,000 or 1.4% of annual turnover, whichever is higher. The infringements that give rise to such sanctions include, inter alia, the failure to implement technical and organisational security measures under Article 21 of Directive (EU) 2022/2555; the omission, delay, or falsification of incident notifications under Article 23; and the failure to cooperate with or obstruct the activities of the ACN in the exercise of its investigatory or supervisory powers.

The aforementioned thresholds are not abstract but find immediate concreteness in the enforcement praxis of the ACN, which, in accordance with the criteria set out in Article 83(2) GDPR—applied mutatis mutandis—evaluates, inter alia, the gravity and duration of the infringement, the degree of negligence or intentionality, the actions undertaken to mitigate the damage, previous infringements, and the degree of cooperation with the supervisory authority. The imposition of sanctions may be accompanied by ancillary measures, such as orders to cease processing, mandates to rectify non-compliance, or temporary suspensions of activities affecting critical infrastructure.

Furthermore, the Italian cybersecurity legal order, particularly within the framework of the Perimetro di Sicurezza Nazionale Cibernetica established under Decree-Law no. 105 of 21 September 2019, includes penal provisions. Specifically, non-compliance with ministerial or ACN orders issued pursuant to Article 1 of the decree may constitute an offence under Article 650 of the Italian Criminal Code, punishable by arrest or pecuniary fine, without prejudice to more serious offences relating to public security, national defence, or state secrets.

The administrative enforcement of cybersecurity

measures is also supplemented by sectoral authorities in specific industries, such as AGCOM for telecommunications, ARERA for energy, and IVASS for insurance, which may impose independent sanctions under lex specialis where the cybersecurity infraction affects regulated services under their respective jurisdictions. In particular, DORA Regulation (EU) 2022/2554, as supplemented by Delegated Regulations 2024/1773 and 2024/1774, introduces further supervisory powers for financial authorities to impose corrective measures, including fines, on entities violating digital operational resilience obligations, which are distinct yet complementary to the ACN's competence under the NIS2 transposition.

In sum, the Italian sanctions regime for cybersecurity violations is characterised by a graduated, inter-authority, and risk-based structure, aligned with European harmonisation imperatives, which confers upon the ACN and ancillary sectoral regulators a broad discretionary arsenal for ensuring compliance, preserving national security, and deterring recidivism, through both administrative coercion and, where warranted, penal recourse.

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

Yes, the imposition and quantification of administrative sanctions for cybersecurity-related breaches within the Italian jurisdiction is subject to a composite set of rules and interpretative guidelines, which, while lacking a codified tariff system, are grounded in European legal standards and systematically applied by national authorities such as the *Agenzia per la Cybersicurezza Nazionale* (ACN), the *Garante per la Protezione dei Dati Personali*, and other competent sectoral regulators.

1. Under the GDPR (for data breaches involving personal data):

Fines are calculated according to **Article 83 GDPR**, which establishes two tiers: – Up to €10 million or 2% of the global annual turnover (for breaches of obligations such as security measures or failure to notify); – Up to €20 million or 4% of the global annual turnover (for breaches of data processing principles, data subject rights, or cross-border transfer rules).

The *Garante per la Protezione dei Dati Personali* applies a **contextualised assessment** based on the ten criteria set out in **Article 83(2) GDPR**, including: – Nature, gravity, and duration of the infringement; – Intentional or negligent character; – Mitigating actions and degree of cooperation; – Categories of personal data involved; – Past infringements and repetition; – Financial gain from the infringement.

These criteria are applied **cumulatively** and result in a **graduated sanction**, often scaled in proportion to the infringer's economic capacity. The *Garante* follows the **EDPB's Guidelines 04/2022** on administrative fines, using a five-step methodology to identify the base amount and apply contextual adjustments.

2. Under NIS2 and Legislative Decree No. 138/2024:

Article 34 of D.Lgs. 138/2024, transposing **Articles 34–36 of the NIS2 Directive**, empowers the ACN to impose **graduated fines** on both "essential" and "important" entities for: – Failing to implement risk management measures; – Not notifying incidents within statutory timeframes; – Obstructing supervisory activities.

The maximum administrative fines mirror the GDPR's structure: – Up to €10 million or 2% of global annual turnover for breaches of incident notification or risk management duties; – The fine must be "effective, proportionate, and dissuasive", as per **Article 34(1) D.Lgs. 138/2024**.

While no binding guidelines on fine calculation have yet been issued by the ACN, the Determination No. 38565/2024 and upcoming sector-specific decrees anticipate the use of **risk-based and size-adjusted criteria**, likely mirroring the EDPB model, incorporating sectoral criticality and severity of impact.

3. Under the PSNC regime (D.L. 105/2019 and DPCM 131/2020):

Entities designated within the *Perimetro di Sicurezza Nazionale Cibernetica* may be sanctioned by the ACN for: – Non-implementation of prescribed security measures; – Failure to register ICT assets; – Omission or delay in incident notification.

The **sanctions can include**: – Monetary fines (scalable based on the strategic relevance of the asset); – Suspension from public procurement; – Injunctions or technical corrective orders.

The **ACN has discretion** in calibrating the sanction based on the entity's size, the systemic risk posed, and any aggravating or mitigating circumstances.

4. Under DORA (from January 2025):

Regulation (EU) 2022/2554 (DORA) does not set uniform

fine amounts but requires competent financial supervisors (e.g., *Banca d'Italia*, *CONSOB*) to adopt sanctions that are "effective, proportionate and dissuasive". Thresholds are set according to sectoral laws (e.g., TUF, TUB) but aligned with the severity of ICT incidents and operational failures.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, in the Italian legal system, **enforcement decisions issued pursuant to cybersecurity laws**—whether by the *Agenzia per la Cybersicurezza Nazionale (ACN)*, sectoral authorities such as the **Bank of Italy**, **CONSOB**, **AGCOM**, **ARERA**, or by the **Garante per la Protezione dei Dati Personali** in the case of data security obligations—are subject to **judicial review and appeal**, in accordance with the constitutional principles of due process and administrative legality.

1. Appeals Against ACN Enforcement Decisions

Enforcement measures issued by the **ACN** under **Legislative Decree No. 138 of 4 September 2024** (implementing the **NIS2 Directive**)—such as injunctions, fines, suspension orders, or certification revocations—are **administrative acts** subject to appeal before the **Tribunali Amministrativi Regionali (TAR)**, and in particular, the **TAR Lazio (Rome)** when the act is national in scope or issued by central administration.

The relevant procedural framework is governed by the **Codice del Processo Amministrativo (Legislative Decree No. 104/2010)**. The appeal must be filed within **60 days** of notification or publication of the contested act and may seek:

– **annulment** of the administrative act for illegality, excess of power, or procedural violation; – **suspension (injunction)** of enforcement pending judgment; – **compensation for damages** suffered as a result of the unlawful act.

The TAR's judgment may be **further appealed to the Consiglio di Stato**, Italy's supreme administrative court, within **30 days** from notification of the first-instance judgment.

2. Appeals Against Enforcement in the Financial Sector (DORA)

Sanctions and remedial measures imposed under **Regulation (EU) 2022/2554 (DORA)** by financial regulators such as the **Bank of Italy**, **CONSOB**, or **IVASS**, are typically challenged before the **ordinary civil courts**, unless the enforcement action takes the form of a public law act or impacts a licence, in which case administrative jurisdiction may apply.

Specific recourse mechanisms are defined by the sectoral laws applicable to supervised entities. For instance:

– **Administrative fines** may be appealed before the **TAR** within 60 days; – **Private law measures** (e.g., exclusion from critical ICT services) may be appealed before the **Tribunale Ordinario** under **summary cognizance procedures**.

Moreover, judicial remedies must ensure the effective protection of the rights guaranteed by EU law, including the right to a fair hearing, proportionality, and the right to an effective remedy under **Article 47 of the EU Charter of Fundamental Rights**.

3. Appeals Against Garante Data Security Measures (GDPR)

Where a cybersecurity enforcement measure is issued by the **Garante per la Protezione dei Dati Personali**, particularly in relation to Article 32 GDPR or security breach obligations, appeal lies with the **ordinary civil courts** pursuant to **Article 152 of the *Italian Privacy Code***.

Such proceedings are brought before the **Tribunale Civile**, typically in Rome, under **summary procedure (rito sommario di cognizione)**, with full adversarial rights and the possibility of **suspensive measures** pending final adjudication.

Further appeal lies to the **Corte d'Appello**, and ultimately to the **Corte di Cassazione** on points of law.

4. Appeals Against ACN Measures under the Cybersecurity Perimeter

Entities subject to the **National Cybersecurity Perimeter** (Law No. 133/2019; DPCM No. 131/2020) and impacted by ACN's strategic measures—such as removal of ICT assets, exclusion from procurement, or classification of vulnerabilities—may also seek redress before the **TAR**, applying administrative review standards, including proportionality, manifest error, and violation of legitimate expectations.

Given the **classified nature of many perimeter-related decisions**, proceedings may be subject to **procedural confidentiality**, and appeals may require specific standing or security clearance, especially where national defence is implicated.

5. EU-Level Review of Enforcement Decisions

In cross-border cases governed by **DORA**, **GDPR**, or **NIS2**, where a binding decision is issued through a European supervisory mechanism (e.g., under Article 65 GDPR or Article 31 DORA), appeal may lie before the **General Court of the European Union** pursuant to **Article 263 TFEU**, subject to standing and admissibility conditions.

This includes cases where Italian authorities act under delegated EU law or implement decisions adopted by the European Supervisory Authorities or the European Data Protection Board.

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

An analysis of the prevailing enforcement orientation in the Italian jurisdiction during the biennium 2024–2025 reveals an intensified supervisory commitment toward the prevention, detection, and sanctioning of systemic deficiencies in cybersecurity governance, particularly in those domains delineated by supranational instruments as being of strategic relevance to national security and public order. The Agenzia per la Cybersicurezza Nazionale (ACN), acting in its dual capacity as National Competent Authority under the NIS2 transposition and as operational coordinator within the Perimetro di Sicurezza Nazionale Cibernetica, has inaugurated an enforcement paradigm premised not merely on reactive sanctioning but on anticipatory resilience verification, scenario-based testing, and sectoral maturity assessment.

The investigatory focus has gravitated toward entities whose ICT assets are classified as critical for the maintenance of essential societal or economic functions, with particular vigilance directed to energy distribution, digital infrastructure, telecommunications, and public administration domains. Inspections have targeted the substantive adequacy of implemented security measures under Article 21 of Directive (EU) 2022/2555 and their conformity with the minimum requirements set forth in the Regolamento di Esecuzione (UE) 2024/2690, including the effective separation of duties, incident detection capabilities, encryption safeguards, and the traceability of security events.

Concurrently, the ACN has shifted its enforcement lens toward the phenomenon of supply chain vulnerability, compelling regulated entities to demonstrate the integration of third-party ICT risk management policies as prescribed by DORA and its implementing regulations. This shift has been accompanied by a regulatory intolerance toward superficial compliance documentation, with the ACN rejecting risk assessments and registers that fail to establish material congruence between theoretical models and actual technological deployments.

Of equal salience is the regulatory intolerance for incident underreporting or delay in mandatory notification. Enforcement activities during the reporting period have underscored the punitive treatment of entities failing to notify significant incidents within the prescriptive temporal thresholds. In such cases, ACN has combined pecuniary sanctions with injunctive mandates and public disclosure, thus reinforcing the deterrent function of transparency.

Finally, the publication of the 2025 National Cybersecurity Strategy has established the governance of AI-based cyber defences and the institutionalisation of threat intelligence sharing as emergent priorities, with enforcement resources being realigned toward ensuring the operationalisation of these axes. The convergence of data protection and cybersecurity enforcement has intensified, with cross-institutional inspections conducted in synergy with the Garante per la Protezione dei Dati Personali, especially in cases where security breaches implicate personal data and digital identity systems.

Thus, the regulatory posture adopted by the Italian cybersecurity authority is characterised by anticipatory control, sectoral stratification, and a formalised risk proportionality analysis, embedded within a doctrine that privileges traceability, accountability, and continuous improvement over mere formalistic adherence to statutory text.

Contributors

Luca Bolognini
Founding Partner
luca.bolognini@ictlc.com

Paolo Balboni
Founding Partner
paolo.balboni@ictlc.com

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

Nicolò Maria Salvi
Partner
nicolo.salvi@ictlc.com