Italy

Diego Rigatti and Pietro Giorgio Castronovo
Orrick, Herrington & Sutcliffe

www.practicallaw.com/9-502-4794

REGULATION

1. What national law(s) regulate the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

Legislative Decree of 30 June 2003 No. 196 (the Code concerning the protection of personal data) (Code) applies in Italy. The Code implements both:

- Directive 95/46/EC on data protection (Data Protection Directive).
- Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive).

2. To whom do the rules apply (EU: data controller)?

The Code applies to any data controller, that is, any individual or legal person (including public bodies) who is competent to determine the purposes, methods and instruments of processing of personal data (including security matters). In addition, the data controller can process the data jointly with another data controller.

3. What data is regulated (EU: personal data)?

Personal data means information which can identify any individual or legal person, even indirectly by reference to other information, including a personal identification number. The Code also regulates (with stricter rules) sensitive data and judicial data (*see Question 11*).

4. What acts are regulated (EU: processing)?

The Code applies to personal data processing, that is, any operation, or set of operations, carried out with or without electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilisation, interconnection, blocking, communication, dissemination, deletion and destruction of data, whether or not it is contained in a data bank.

5. What is the jurisdictional scope of the rules?

The Code applies to any individual or legal person established in Italy's territory, or in a place under Italy's sovereignty, performing personal data processing, including of data held abroad.

The Code also applies to personal data processing by any entity established outside the EU using equipment in Italy's territory, electronic or otherwise, unless the equipment is only used for transit through the EU. If it applies, the Code requires the appointment of a national representative to apply Italian laws on data protection.

6. What are the main exemptions (if any)?

The Code does not apply to processing carried out by individuals exclusively for personal purposes, unless the data is to be systematically communicated or disseminated.

7. Is notification or registration required before processing data? If so, please provide brief details.

Notification of processing is generally not required. Notification to the Data Protection Authority (*see box, The regulatory authority*) is required only in the following cases (*Code*):

- Genetic data, biometric data or other data disclosing the geographic location of individuals or objects through an electronic communications network.
- Data disclosing information about health and sex life, where it is processed for the purposes of any of the following:
  - assisted reproduction;
  - provision of healthcare services through electronic networks in connection with data banks and/or the supply of goods;
  - epidemiological surveys;
  - diagnosis of mental, infectious and epidemic diseases;
  - HIV status;
  - organ and tissue transplantation; and
  - monitoring of healthcare expenditure.
- Data disclosing sex life and the psychological sphere, where it is processed by not-for-profit organisations, of a political, philosophical, religious or trade union character.

- Data processed with the help of electronic means, aimed at:
  - profiling the data subject and/or his personality;
  - analysing consumption patterns and/or choices; or
  - monitoring use of electronic communications services.

  This does not apply to processing operations that are technically indispensable to deliver these services to users.
- Sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys.
- Data stored in data banks managed by electronic means, in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

The Data Protection Authority can specify, through specific decisions, further operations that are liable to affect data subjects' rights and which require notification.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

Data controllers have the following main obligations:

- To provide information on the processing to data subjects (*see Question 12*).
- To obtain consent from data subjects, unless an exemption applies in the Code (*see Question 9*).
- To adopt proper security measures and to update them periodically (*see Question 14*).
- To file a notification to the Data Protection Authority where necessary (*see Question 7*).
- To help uphold data subjects' rights, as provided for in the Code (*see Question 13*).
- For data processing by means of electronic instruments, to identify and instruct in writing one or more system manager(s) (*Amministratore di Sistema*) (the person(s) managing the data controller's IT systems).

9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there concerning the form and content of consent? Does online consent suffice?**
- **Are there any special rules concerning consent by minors?**

The Code generally requires express consent. Consent must be documented in writing (which includes online consent), but can be granted orally if noted in writing by the controller.

Written consent is required for sensitive data processing, and online consent is insufficient, unless a certified digital signature is provided (*Code*).

There are no specific data protection rules concerning consent given by minors (individuals under the age of 18). General principles of Italian law apply:

- Consent granted by minors is invalid, as consent can only be granted by a person with full legal capacity. There is an exception where it is proved the minor had the ability to understand the consequences of his consent.
- The parents of a minor can give their consent to processing the minor's data.

10. If consent is not given, on what other grounds (if any) can processing be justified?

General exemptions

Consent is not required where processing:

- Is necessary to comply with an obligation imposed by a law, regulations or EU legislation.
- Is necessary to execute contracts to which the data subject is a party, or else to comply with specific requests made by the data subject before entering into a contract.
- Concerns data taken from publicly available registers, lists, documents or records, without prejudice to the limitations and modalities laid down by laws, regulations and EU legislation regarding their disclosure and publicity.
- Regards data relating to economic activities, that is processed in compliance with business and industrial secrecy legislation.
- Is needed to safeguard a third party's life or integrity.
- Is required to carry out investigations by defence counsel, or to establish or defend a legal claim.
- Is necessary to pursue a legitimate interest of either the data controller or a third-party recipient, certain cases specified by the Data Protection Authority on the basis of the principles set out under the law, including certain activities of banking groups and subsidiaries or related companies, unless this interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests.
- Is carried out by non-profit associations, bodies or organisations (but not for the purpose of external communication and dissemination).
- Is exclusively necessary for scientific and statistical purposes in compliance with the relevant codes of professional practice.

Direct marketing and telemarketing

In general, the data in telephone subscriber directories can be processed lawfully for further purposes, including advertising, promotional and/or commercial purposes. This is provided the data subjects have given their informed, free and specific consent, which must be documented in writing.

However, the processing for phone marketing purposes of data in public telephone directories or other publicly available databases is forbidden if the relevant persons or entities have registered in a specific opt-out register (*section 130, Par. 3-bis (Act No. 166 of 20 November 2009)*).

Whistleblowing

The situation concerning whistleblowing is unclear. According to a recent report issued by the Data Protection Authority on a strict interpretation of the privacy laws, the data subject must consent to the processing of his data for whistleblowing purposes.

In particular, the Data Protection Authority pointed out that the:

- Processing of personal data in the context and for the purpose of whistleblowing should be performed after having obtained the data subject's consent, because there are no clear rules affirming that whistleblowing is a legal mandatory obligation where the data subject's consent is not required (*see above, General exemptions*).
- Data subject has the right to know the source of the personal data (*see Question 13*).

However, other legal rules might help companies justify adopting a whistleblowing procedure, which does not require the data subject's previous consent. These include:

- Legislative Decree No. 231/2001 on the direct liability of legal entities for crimes committed by directors, executives, their subordinates, agents and others acting on behalf of the legal entity.
- Article 2105, Italian Civil Code, on employees' duty of loyalty.

These rules protect the general interests of the market (in other words, the financial market's stability, punishment of economic and financial crimes or corruption, protection of stakeholders, and compliance of companies with rules avoiding criminal liability), as well as the company's internal interests (for example, employees' infidelity).

Given the uncertainty of this area, the Data Protection Authority has asked the Parliament to provide specific rules.

11. Do special rules apply for certain types of personal data, for example sensitive data? If so, please provide brief details.

Special rules apply to sensitive data, that is, personal data involving the disclosure of any of the following:

- Racial or ethnic origin.
- Religious, philosophical or other beliefs.
- Political opinions, or membership of parties or trade unions, associations or organisations of a religious, philosophical, political or trade union character.
- Health and sex life.

Sensitive data can only be processed:

- With the data subject's written consent.
- With the Data Protection Authority's authorisation.
- By complying with the requirements and limitations set out in the Code, and other laws and regulations.

The Data Protection Authority has issued general authorisations (which are renewed on a yearly basis) allowing sensitive data processing by certain categories of individuals or entities (such as doctors, lawyers and public bodies) or for certain purposes (such as recruitment or employment purposes).

Special rules also apply to judicial data, that is, personal data disclosing the:

- Restrictive measures marked in the criminal record office and in the register of administrative fines related to criminal offences and relevant pending charges.
- Identity of the defendant or person that is subject to investigation under the Code of Criminal Procedure.

Judicial data processing by private entities and profit-seeking public bodies is only permitted where expressly authorised by a law or an order by the Data Protection Authority, specifying the:

- Public interest reasons for the processing.
- Categories of processed data.
- Operations that may be performed.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

Data subjects must be provided with a notice containing the following information (as a minimum), at the time of collection or, in any event, before data processing:

- The purposes and modalities of the processing, in that the data is:
  - processed lawfully and fairly;
  - collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with these purposes;
  - accurate and, when necessary, kept up to date;
  - relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
  - kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.
- Whether providing the requested data is obligatory or voluntary.
- The consequences of refusing to provide data.
- The entities, or categories of entities, to whom the data can be communicated or that may come to know the data due to their appointment as processor or person in charge of processing.
- The data subject's rights under the Code.
- Identity of the data controller or, if appointed, of the national representatives of the controller and processor.

The same notice must be provided by a controller who has collected data from third parties, at the time of collection or registration of the data or, if data is to be communicated, no later than the first communication.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

Data subjects are entitled to obtain confirmation that their data exists in a clear and intelligible way. They are also entitled to the following information:

- The source of the data.
- The purposes and form of the data processing.
- The logic applied to the processing carried out electronically.
- Details of the controller, its national representative (if appointed) and the data processor.

- Entities, or categories of entities, to which the data can be communicated or that may come to know the data due to their appointment as processor or person in charge of processing.

Data subjects are also entitled to demand:

- The update, rectification or integration of their data.
- The cancellation, anonymisation or blocking of data that has been processed unlawfully, including data the retention of which is unnecessary for the purposes for which it has been collected or subsequently processed.
- Certification of the fact that these operations have been notified, and of the contents of notified operations, to the entities to which the data was communicated or disseminated.

Data subjects can oppose their data being processed if they have legitimate grounds and, in any event, if the processing is for direct marketing purposes.

SECURITY REQUIREMENTS

14. What security requirements are imposed in relation to personal data?

Generally, personal data must be kept and controlled to minimise risks of loss and destruction, by using suitable preventative security measures.

The Code provides for specific minimum security measures to be adopted to ensure a minimum level of data protection. These minimum security measures are listed in Annex B to the Code and they include:

- Using ID and passwords with certain characteristics.
- Using firewalls meeting certain requirements.
- Adopting a security policy document by 31 March of each year, as a result of a thorough analysis of the potential risks that might occur in personal data processing by the controller.

PROCESSING BY THIRD PARTIES

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

If a third party processes data on the data controller's behalf, it should be appointed as data processor. The data processor is an individual or entity that ensures compliance with data protection provisions who is appointed on the basis of on capacity, experience and reliability.

The processor acts according to written instructions provided by the controller, who is liable for the supervision of the processor's activities and carries out periodical inspections to ensure the processor complies with the controller's instructions. The data controller must also evaluate whether it is appropriate to additionally instruct the third party as system manager (for example, if the third party provides the data controller with IT services and manages the data controller's IT systems).

THE REGULATORY AUTHORITY

Data Protection Authority (*Garante per la Protezione dei Dati Personali*)

W *www.garanteprivacy.it*

Main areas of responsibility. Surveying and enforcing compliance with the Code and maintaining the register of notification.

INTERNATIONAL TRANSFER OF DATA

16. What rules regulate the transfer of data outside your jurisdiction?

The transfer of data to other EU member states is allowed. The Code expressly states that its provisions do not limit the free circulation of personal data within the EU.

The transfer of data to non-EU countries is admitted where the data subject has given its consent, and in a number of other cases where exemptions similar to those listed in *Question 10* apply.

In addition, transferring data to non-EU countries is allowed if this is either:

- Authorised by the Data Protection Authority, either:
  - in connection with contractual safeguards; or
  - under rules of conduct adopted within a group of companies.
- Based on decisions taken by the European Commission (Commission) according to sections 25(6) or 26(4) of the Data Protection Directive, under which a non-EU country is deemed to grant an adequate level of protection or a determined set of contractual clauses affording sufficient safeguards.

17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The Data Protection Authority has ratified, with specific decisions, both the standard controller-to-controller agreement and the standard controller-to-processor agreement as approved by:

- Decision 2004/915/EC on an alternative set of standard contractual clauses for the transfer of personal data to third countries (Data Controller Contractual Clauses Amendment Decision).
- Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in third countries (Data Processor Contractual Clauses Decision).

18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

If a transfer agreement complies with the standard agreement as approved by the Commission, then specific consent to that transfer need not be requested (*Code*) (*see Question 17*). However, all other requirements should be met, for example:

- The information notice should be provided (*see Question 12*).
- Consent to the processing (if requested) should be obtained (*see Question 9*).

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

If a data transfer agreement does not comply with the standard agreement approved by the Commission, then the parties to the agreement must submit the agreement to the Data Protection Authority for its approval.

ENFORCEMENT AND SANCTIONS

20. What are the enforcement powers of the national regulator?

The Data Protection Authority supervises personal data processing carried out with powers granted by the Code.

The most relevant enforcement powers are as follows:

- Receiving reports and complaints from data subjects or their associations, and taking appropriate steps in relation to these.
- Ordering data controllers, also *ex officio*, to take necessary or appropriate measures to comply with the provisions in force.
- Prohibiting, also *ex officio* (by virtue of office), unlawful or unfair data processing.

21. What are the sanctions and remedies for non-compliance with data protection laws? To what extent are the laws actively enforced?

There are administrative and criminal sanctions for non-compliance with the Code, and an interested party can sue the data manager responsible for the illegal behaviour to recover damages.

Breach of administrative rules

The following fines apply for breach of administrative rules:

- Non-provision or provision of an incomplete information notice to data subjects: a fine from EUR6,000 (about US$8,090) to EUR36,000 (about US$48,546).
- Processing data without adopting the minimum security measures under the Code or unlawful data processing (which is also a crime; *see below, Criminal offences*): a fine from EUR10,000 (about US$13,485) to EUR120,000 (about US$161,819).
- Failure to submit notification or submitting an incomplete notification to the Data Protection Authority: a fine of EUR20,000 (about US$26,969) to EUR120,000.
- Breach of provisions on retraining traffic data (unless the facts at issue are deemed to be criminal offences): a fine from EUR10,000 to EUR50,000 (about US$67,424).
- Failure to provide information or documents to the Data Protection Authority: a fine from EUR10,000 to EUR60,000 (about US$80,909).

Criminal offences

The following sanctions apply in relation to various criminal offences:

- Unlawful data processing (for example, carried out without the data subject's consent) where damage has been caused to a third party: imprisonment for between six and 18 months.
- Unlawful data processing, if the offence consists of data communication or dissemination: imprisonment for between six and 24 months.
- Other cases of unlawful data processing (such as processing sensitive data without the data subject's consent or unlawful international transfer of data): imprisonment for between one and three years.
- False declaration or notification to the Data Protection Authority: imprisonment for between six months and three years.
- Failure to adopt the minimum security measures under the Code: imprisonment of up to two years.
- Failure to comply with decisions issued by the Data Protection Authority: imprisonment for between three months and two years.

For criminal offences, the legal representatives of the entity acting as data controller or processor bear liability.

CONTRIBUTOR DETAILS

Diego Rigatti
Orrick, Herrington & Sutcliffe
T +39 02 4541 3861
F +39 02 4541 3801
E *drigatti@orrick.com*
W *www.orrick.com*

Areas of practice/expertise. Diego Rigatti, a partner in the Milan office, is a member of the firm's European Corporate and Intellectual Property Groups. Mr Rigatti has extensive experience in intellectual property, privacy, IT and e-commerce services. His current clients include leading banks and financial institutions, global retail companies and social networks.

Mr Rigatti is a frequent lecturer in various congresses on data protection and privacy, intellectual property, e-commerce and related matters. He was also selected as an external expert by to review the reports issued during the UE START Programme (a programme on e-commerce development within European companies), by the Ministry of Finance to participate in a multidisciplinary commission on the internet economy, and by Regione Lombardia to lead a joint venture between Banca Intesa, Ernst & Young, Poste Italiane and others to sponsor and support a regional e-commerce incentive campaign among the small- and medium-sized companies in Lombardy.

Pietro Giorgio Castronovo
Orrick, Herrington & Sutcliffe
T +39 02 4541 3861
F +39 02 4541 3801
E *pcastronovo@orrick.com*
W *www.orrick.com*

Areas of practice/expertise. Pietro Giorgio Castronovo, an associate in Orrick's Milan office, is a member of the European Corporate Group.

Mr Castronovo's practice focuses on cross-border transactions and strategic alliances for domestic and international clients, technology agreements, commercial agreements, intellectual property law and privacy law.