DATA PROTECTION LAWS OF THE WORLD

Italy

ITALY

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Italian data protection law framework has been harmonized with the GDPR by means of the Legislative Decree 101 /2018, that entered into force on 19 September 2018, and amended a number of provisions of the Legislative Decree 196 /2003 (the "**Privacy Code**"), as well as introduced some transitional provisions regulating the migration to the new regime.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Italian Privacy Code adopts the definitions provided by the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Privacy Code provides that the supervisory authority in Italy is the Garante per la protezione dei dati personali (the “**Garante**”). The Garante is composed of a Council and an Office. The Council is made up of four members, two elected by the Chamber of Deputies and two by the Senate of the Republic. The members are elected amongst those who apply for this position in a selection procedure whose details are published on the websites of the Chamber of the Deputies, the Senate of the Republic and the Garante. The members elect a Chairman, in the event of parity of votes. Law Decree 139/2021 (so-called “Decreto Capienze”) introduced an important change to the number of Garante’s members, which, starting from January 1st, 2022, increases from 162 to 200 members, recruited by way of a public competition.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of

personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the GDPR and the Privacy Code there is no obligation to notify regulators of any data processing activity.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;

- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by EU or Member State law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Act

The Regulation on harmonized rules on fair access to and use of data (Data Act) has been approved on January 11th 2024. This regulation puts obligations on manufacturers and service providers to let their users, both companies and individuals, access and reuse data generated by the use of their products or services and share such data to third parties. It also improves data portability in all economic sectors.

Article 2-*ter* of the Privacy Code (as amended by Law Decree 139/2021) provides that, in case of processing of personal data for reasons of public interest or in connection with the exercise of public powers, the legal basis may also derive from a general administrative act. In such cases where it is necessary to disseminate or communicate personal data to other subjects for reasons of public interest or in connection with the exercise of public powers, it will be required to notify the Garante at least 10 days before the start of the communication or dissemination.

Furthermore, since Law Decree 139/2021 repealed Article 2-*quinquiesdecies*, the Garante is no longer entitled to prescribe the data controller to adopt measures and precautions to safeguard the data subjects for data processing that pose a high risk for the same, in case of processing of personal data performed for reasons of public interest or in connection with the exercise of public powers.

Article 2-*sexies* of the Privacy Code specifies that the processing of special category data necessary for the performance of a task carried out in the public interest is allowed insofar as the processing is provided for by European or domestic legislation, or, as recently introduced by the Law Decree 139/2021, by a general administrative act. This legislation must identify the reasons of public interest for which the processing is carried out, the types of data that can be processed, the operations that can be performed and the appropriate and specific measures protecting the fundamental rights and interests of the data subjects. In this context, the Privacy Code underlines that processing of genetic data, biometric data or data concerning health shall comply with additional requirements to be identified by the Garante by means of specific measures establishing further conditions in which the data processing is permitted.

With regard to personal data relating to criminal convictions and offences, Article 2-*octies* of the Privacy Code provides that the processing can be carried out only if a specific legal provision authorizes the processing, also identifying the applicable security measures, otherwise processing activities have to be carried out under the control of a public authority.

With regard to individuals’ rights, Art. 2-*undecies* of the Privacy Code provides several restrictions on data subjects’ rights for reasons of justice. In particular, data subjects rights may be exercised within the limits established in the law and regulations on the proceeding and procedures before the courts. The exercise of such rights may be delayed, limited or excluded for as long as and to the extent that it is a necessary and proportionate measure, having regard to the fundamental rights and legitimate interests of the data subject. Finally, the Privacy Code sets out data protection rights of deceased persons. Indeed, the rights provided for in Articles 15 through 22 of the GDPR referring to personal data concerning deceased persons may be exercised by those having an interest of their own, or act to protect the data subject, as her / his delegate, or for family reasons worthy of protection. The exercise of such rights is not permitted when provided for by the law or when, specifically limited to the offer of information society services, the data subject expressly prohibited it in writing by way of a declaration sent to the data controller. The data subject may withdraw or modify such declaration at any time.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

On July 10, 2023, the EU Commission adopted an adequacy decision pursuant to art. 45 of the GDPR. In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework ("DPF") and has decided that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the DPF.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Privacy Code does not derogate from the GDPR in regard to transfers.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Privacy Code does not prescript further security measures that should be followed to protect personal data.

Nevertheless, genetic data, biometric data or data concerning health must be processed in accordance with the additional safeguard measures issued by the Garante every two years (Article 2-*septies*). Such safeguard measures take into account the guidelines, recommendations and best practices published by the European Data Protection Board and best practices on personal data processing; scientific and technological evolution in the sector covered by such measures; and the interest of the free flow of personal data within the territory of the Union. Also, the Garante may issue codes of ethics that set out security measures for the processing of personal for statistical and scientific research purposes.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*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*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

In the new version of the European Data Protection Board Guidelines 09/2022 issued on March 28, 2023, the EDPB specified the mere presence of a representative of a data controller not established in the EU does not trigger the one-stop-shop system. Therefore, the data breach shall be notified to every supervisory authority for which affected data subjects reside in their Member State.

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Privacy Code does not set out additional rules on data breach notifications.

However, data breaches that require notification should be notified to the Garante by completing a form available at the Garante website. The notification form, once completed with the required information, must be sent via certified e-mail to the Garante and must be signed digitally (with qualified electronic signature / digital signature) or with handwritten signature.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Privacy Code provides that investigations and enforcement actions handled by the Garante.

ELECTRONIC MARKETING

The GDPR and the Privacy Code apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). As further analyzed below, under Section 130 of the Privacy Code, the legal basis for electronic marketing is consent. The strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Privacy Code (Section 130) does not prohibit the use of personal data for the purpose of electronic marketing, but it requires the prior informed consent (opt-in) from the recipient of the communication. The use of automated calling or communications systems without human intervention for the purposes of direct marketing or for sending advertising materials, or else for carrying out market surveys or interactive business communication, as well as electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means shall only be allowed with the contracting party’s or user’s consent. Such consent shall be recorded with reference to its date and the person giving it in order to be used as evidence of the consent.

Separate consents shall be required for the registration to a website and the opt-in to the delivery of marketing communications, however the data subjects may be required to provide a unique marketing consent covering the different marketing practices (e.g. marketing via SMS, email, telephone, market surveys, etc.) performed through the collected data, provided that such practices are outlined in the information notice provided to data subjects.

An additional separate consent shall be required for the transfer of collected personal data to third parties for marketing purposes. Said third party shall also be identified at least on the basis of its category of operation and provide an information notice to data subjects before the delivery of marketing communications.

Where a data controller uses, for direct marketing of his own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject’s consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes here referred.

Electronic marketing communications shall clearly identify the sender and provide to the recipient all necessary information in order for him / her to eventually refuse the delivery of the direct marketing material (*opt-out*).

The possibility for the recipient to opt-out from marketing communication services must be guaranteed both during the first contact with the recipient and during any following communications.

Marketing communications by way of non-automated telephone calls are permitted provided that either:

- the data subject has given his prior consent, if there is an ongoing relationship that has not expired for more than 30 days; or
- the number (that can now also be a mobile number) of the data subject is included in the telephone directory and (s)he has not entered in a public opt-out register ("*Registro delle Opposizioni*") and opted out from being contacted for marketing purposes.

Law 11 January 2018, no. 5 provides stringent rules on telemarketing, including, amongst others, the withdrawal from all consents previously given in case of enrolment in the *Registro delle Opposizioni*, save for consents provided based on contractual arrangements in place or expired less than 30 days before the enrolment, and the prohibition to communicate, transfer or disseminate personal data related to data subjects registered in the *Registro delle Opposizioni* for advertising or sales purposes or for the purposes of carrying out market research or commercial communications not related to the activities, products or services offered by the data controller.

On March 24, 2023 the Garante approved a Code of Conduct for telemarketing and teleselling activities (*Codice di condotta per le attività di telemarketing e teleselling*), which is a self-governance instrument that contributes to the correct application of telemarketing regulations and to the dissemination of consumer protection principles and measures among call centres and other operators in the sector. This Code of Conduct applies to all operators that carry out activities of promotion and / or offer of goods and services by telephone to persons on Italian territory that can adhere to it on a voluntary basis. The Code of Conduct envisages several obligations - not strictly related to personal data protection – to which those engaged in telemarketing / teleselling activities must comply with, such as (i) register with the Register of Communications Operators ("**ROC**") and use only the numbers registered with the ROC; (ii) notify the Italian Ministry of Economic Development, Ministry of Labor, National Labor Inspectorate and the Italian Data Protection Authority in case of relocation to a non-EU country (and inform the user at the beginning of the call); and (iii) present the calling line using an appropriate prefix code (or using a number without a code as long as it is registered with the ROC and can be redialed).

The above mentioned privacy provisions apply also to communications sent through private messages on social networks and through *Voip*. On the contrary, should the data subject be a follower of a social network page, it may be implied that the data subject has consented to the delivery of marketing communications of the page. Marketing messages concerning a given brand, product or service as sent by the company managing the relevant social network page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the relevant social network, also based on the information provided, that the recipient did intend in this manner to also signify his / her intention to consent to receiving marketing messages from the given company. However the delivery of marketing communications shall stop when the data subject unregisters from the page.

The Privacy Code provisions relating to marketing and commercial communications make reference to the ‘contracting party’s and user’s consent’ rather than to the ‘data subject’s consent’, referring both to individuals and companies.

ONLINE PRIVACY

The Privacy Code regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.

According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her / his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party’s or user’s computer is only allowed if said contracting party or user has been properly informed and (s)he has given her / his consent.

In July 2021, the Garante released a new set of guidelines for the use of cookies and other tracking tools which introduce a number of new provisions (“**New Cookie Guidelines**”). Companies had to comply to the new rules, starting from January 9, 2022. Among other things, the New Cookie Guidelines provide that:

- as a general rule, scrolling or swiping a page is not considered a valid mechanism to collect the user’s consent, unless it can be proved that scrolling or swiping of the user is the result of an unequivocal choice;
- the request of consent to cookies may not be resubmitted to the user, unless (i) the conditions for processing of personal data significantly change, (ii) it is not possible for the operator of the site to record the previous choice of the user due to a decision of the latter (e.g. deletion of cookies) and (iii) at least 6 months have expired since the previous request;
- the user must be able to continue browsing without being tracked by cookies and he / she must be able to withdraw his / her consent at any time.

With specific reference to the configuration of the cookie banner, the Garante provides that the same shall contain the following elements:

- a command (e.g. an “X” at the top right corner of the cookie banner) which allows the user to close the banner while keeping the default settings and therefore not to give consent to the storing of cookies or the use of other profiling techniques or a command indicating that users continue the navigation of the site without accepting cookie;
- a command to accept all cookies or other tracking tools;
- a short notice on the website’s use of technical cookies and any profiling cookies or other tracking tools, with the relevant purposes;
- a link to the extended cookie policy which indicates any other recipients of personal data, the data retention period and the rights of users; and
- a link to a dedicated area where users can choose, in a granular way, the cookies to be installed with regards to their functionalities, third parties and categories.

Furthermore, the New Cookie Guidelines clarify that a cookie information notice shall be provided:

- in an accessible and simple language;
- which is easily accessible, without discriminations, also to those individuals with disabilities which require them to use assistive technologies and particular configurations;

- also in a multi-layer and multi-channel modality;
- which can be inserted with the website homepage or general privacy information notice, insofar as the website installs technical cookies only; and
- which categorizes cookies and other tracking tools so as to enable distinguishing between technical cookies, analytics cookies and profiling cookies, using a clear, concise and transparent language and layout, insofar as the website installs other categories of cookies than the technical ones.

KEY CONTACTS

Giulio Coraggio
Partner
T +39 02 80 6181
giulio.coraggio@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.