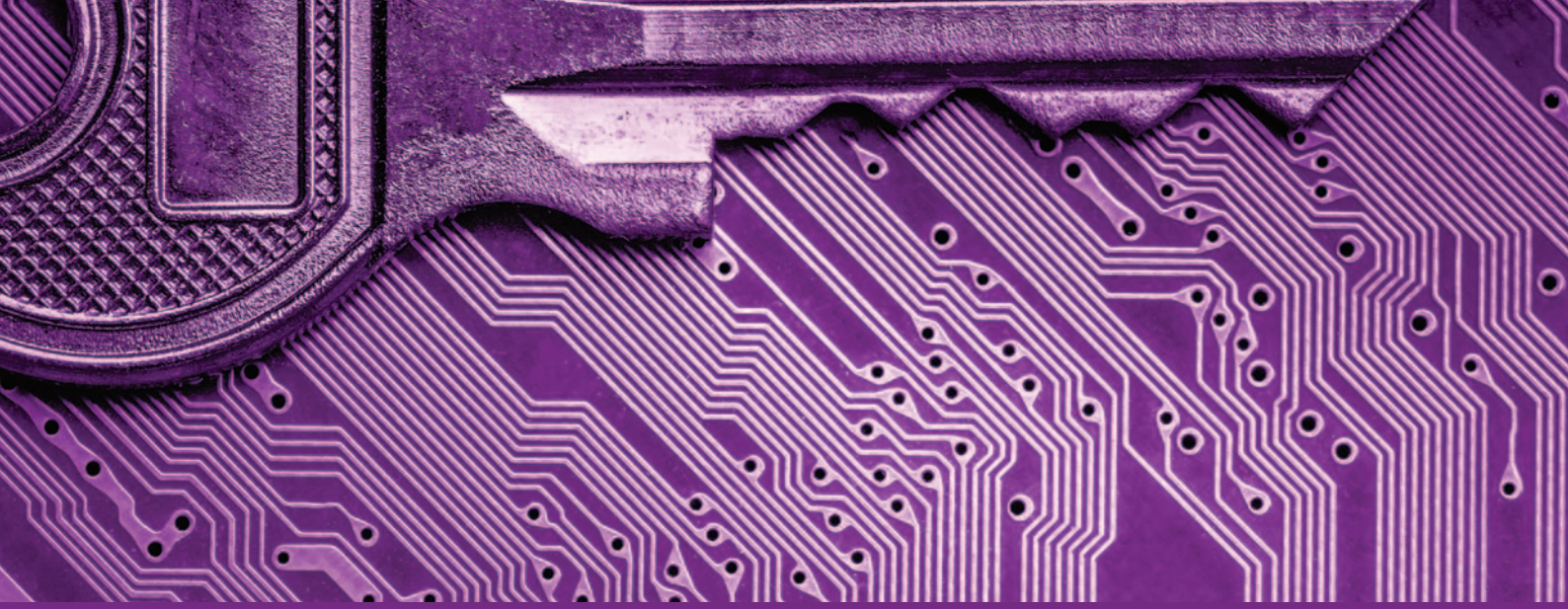

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Italy

Morri Rossetti e Associati – Studio Legale e Tributario

Carlo Impalà

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the main data protection legislation in the EU is Regulation (EU) No. 2016/679 (the "**General Data Protection Regulation**" or the "**GDPR**"). The GDPR repealed Directive 1995/46/EC (the "**Data Protection Directive**") and leads to increased harmonisation of data protection law across the EU Member States.

1.2 Is there any other general legislation that impacts data protection?

The main Italian legislation for the protection of personal data is Legislative Decree 196/2003 (hereinafter the "**Privacy Code**"), recently amended by Legislative Decree 101/2018 in order to adapt it to the changes introduced by the GDPR.

1.3 Is there any sector-specific legislation that impacts data protection?

The following is a non-exhaustive list of the Italian legislation providing for specific rules that impact on data protection:

- L.D. 65/2018 implementing Directive 1148/2016 concerning measures for a high common level of security of network and information systems across the EU;
- L.D. 179/2017 on whistleblowing;
- L.D. 300/1970 (the s.c. "**Statute of Workers**");
- L.D. 81/2008 on health and safety at work;
- L.D. 206/2005 (the s.c. "**Consumers Code**"); and
- Law 5/2018 (the s.c. "**Telemarketing Law**").

The Italian Data Protection Authority regularly issues decisions on specific sectors and data protection issues and, pursuant to Article 22, paragraph 4 of L.D. 101/2018, they will continue to apply as long as they comply with the GDPR and the Privacy Code.

1.4 What authority(ies) are responsible for data protection?

The Italian Authority responsible for monitoring the application of the data protection legislation in force is the "*Garante per la protezione dei dati personali*" (hereinafter referred to as the "**Italian DPA**"). For the performance of its duties, the Italian DPA, where necessary, may avail itself of the collaboration of other Italian authorities or law enforcement agencies (e.g. the "*Guardia di Finanza – Nucleo speciale privacy*" for inspection activities).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  Any information relating to a natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**"

  Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"

  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.
- "**Processor**"

  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 on behalf of the controller.
- "**Data Subject**"

  An individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**"

  Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data (now defined by the GDPR as "**Special categories of personal data**").
- "**Data Breach**"

  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.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  Not applicable.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to:

a) businesses that are established in any EU Member State, and process personal data, either as a controller or processor, and regardless of whether or not the processing takes place in the EU;

b) the processing of personal data by a controller that is not established in any EU Member State, but in a place where Member State law applies by virtue of public international law; and

c) businesses established outside the EU if they (either as controllers or processors) process personal data of data subjects who are in the EU in relation to: (i) the offering of goods or services to such data subjects; or (ii) the monitoring of their behaviour so far as it takes place within the EU.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Personal data must be processed in a transparent manner. Controllers must provide in a concise, transparent, intelligible and easily accessible form, using clear and plain language, certain minimum information to data subjects regarding the processing of their personal data.

- **Lawful basis for processing**

  The GDPR provides for an exhaustive list of legal basis making the data processing lawful, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request; (iii) the controller has a legal obligation, under the EU or any EU Member State laws, to perform the relevant processing; or (iv) the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects.

  Pursuant to Article 9 of the GDPR, the processing of Special categories of personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the processing.

- **Proportionality**

  See answer above under "Data minimisation".

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. Businesses shall take every reasonable step to ensure that inaccurate personal data are either erased or rectified without delay.

- **Retention**

  Personal data must be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Accountability**

  The controller shall be responsible for, and be able to demonstrate compliance with, the GDPR and the applicable data protection law. Businesses shall consider data protection and privacy concerns upfront in any process and operation, also by implementing appropriate technical and organisational measures.

Other key principles – please specify

- **Data protection by design**

  The controller shall, both at the time of the determination of means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.

- **Data protection by default**

  The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only the relevant personal data are processed.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) the categories of data being processed; (iv) the categories of recipients of personal data; (v) the retention period (or the criteria used to determine that period); (vi) the existence of the other rights provided for by the GDPR; (vii) where the personal data were not collected directly from the data subject, the source of such data; and (viii) the existence of, and an explanation of the logic involved in, as well as the envisaged consequences of, any automated decision-making (including profiling) that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data are erased or rectified without undue delay.

- **Right to deletion/right to be forgotten**

  Data subjects have the right to erasure of their personal data if: (i) the data are no longer needed for the original purpose of

processing (and there is not another lawful purpose to process them); (ii) the data subject withdraws consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been unlawfully processed; or (v) erasure is necessary for compliance with EU or Italian law.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the processing is either necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller, or for the purposes of the legitimate interest of the controller or of a third party.

- **Right to restrict processing**

  Data subjects have the right to restrict the processing of personal data, and the controller may hold and use them for limited purposes, if one of the following applies: (i) the accuracy of the data is contested (only for a period enabling the controller to verify that accuracy); (ii) the processing is unlawful; (iii) the controller no longer needs the data for the original purpose of their processing, but the data subject needs to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, following a request to object to processing.

- **Right to data portability**

  Data subjects have a right to receive from the controller a copy of their personal data in a commonly used machine-readable format, and transmit their personal data from this controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**

  Data subjects have the right to withdraw their consent at any time, without affecting the lawfulness of processing made before such withdrawal.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints with the Italian DPA, if the data subjects live in Italy or the alleged infringement occurred in the Italian jurisdiction.

- *Other key rights – please specify*

  Not applicable.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The obligation of prior notification to the Italian DPA, as provided for the processing of "sensitive data" by Article 37 of the former Privacy Code, has been definitely repealed by Article 22, paragraph 8 of L.D. 101/2018.

Only in one case, pursuant to Article 110-*bis* of the Privacy Code (as amended by L.D. 101/2018), third parties willing to reuse personal data for scientific research or statistical purposes must notify the Italian DPA whether, due to particular reasons, the obligation to inform the data subjects is impossible, involves a disproportionate effort, or risks seriously compromising the achievement of such research purposes.

Furthermore, under the GDPR, even if it is not a prior notification, the controller should consult the supervisory authority prior to processing where, as a result of a data protection impact assessment (the "**DPIA**"), that processing would involve a high risk unless the controller implements appropriate measures to mitigate such risk.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable (please see question 6.1 above).

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable (please see question 6.1 above).

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable (please see question 6.1 above).

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable (please see question 6.1 above).

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable (please see question 6.1 above).

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable (please see question 6.1 above).

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable (please see question 6.1 above).

6.9 Is any prior approval required from the data protection regulator?

This is not applicable (please see question 6.1 above).

6.10 Can the registration/notification be completed online?

This is not applicable (please see question 6.1 above).

6.11 Is there a publicly available list of completed registrations/notifications?

The processing register for notifications required under the former Privacy Code is still publicly accessible; however, it has not been updated since 25 May 2018.

6.12 How long does a typical registration/notification process take?

This is not applicable (please see question 6.1 above).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer (hereinafter the "**DPO**") is only mandatory when businesses' core activities consist of data processing which requires: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of special categories of personal data.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Failure to appoint a DPO may result in administrative fines up to €10 million or 2% of worldwide turnover.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

When businesses have appointed a staff member or employee as a DPO, he/she shall not be dismissed or penalised for performing his/her tasks.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO provided that the DPO is easily accessible from each establishment.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO should be appointed on the basis of his/her professional qualities and he/she should have an expert knowledge of data protection laws and practices – which depend on the data processing operations carried out and the protection required for the processed personal data.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO shall be involved in all issues relating to the protection of personal data. The DPO shall, at least: (i) inform the controller, processor and their relevant employees of their obligations under the applicable data protection laws; (ii) monitor compliance with applicable data protection laws and internal policies concerning the protection of personal data; (iii) advise on and monitor the performance of a DPIA; and (iv) co-operate with the relevant supervisory authorities and act as a contact point for the latter and the data subjects on issues related to data processing.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Businesses must notify the contact details of the designated DPO to all the relevant supervisory authorities.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

While the DPO does not necessarily have to be named in a privacy notice, the latter should include the contact details of the DPO. As a matter of good practice, businesses may also inform their employees of the DPO's name.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

A business appointing a processor to process personal data on its behalf is required to enter into an agreement with such processor, which sets out the subject-matter, the duration, the nature and purpose of processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the controller and the processor.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement shall be in writing, executed by both parties, and it must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) commits itself to confidentiality obligations; (iii) ensures the security of the processed data; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in ensuring the rights of data subjects; (vi) assists the controller in ensuring compliance with the GDPR; (vii) either returns or destroys the personal data at the end of agreement (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The legitimate interests of the controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing for direct marketing purposes, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.

However, in the case that the controller uses automated call or call communication systems without the intervention of an operator for advertising or commercial purposes, or to do market research, the recipient must have given her/his prior and express consent. This requirement applies also to processing by means of e-mail, fax, MMS or SMS or others.

The controller shall not request the prior consent of the data subject in order to send communications to promote the sale of its products or services, provided that: (i) the data subject previously purchased similar products or services from such controller; (ii) the communications regard services similar to those purchased; and (iii) the data subject is informed and does not object to such use of his/her data.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The processing of personal data for marketing purposes through phone calls and mail is permitted towards users who have not exercised the right to object, by registering their number and address in the s.c. "Do Not Call" register.

It follows that each controller monthly or, in any case, prior to any advertising campaign, must verify that the user is not listed in the Do Not Call register and update its databases. If he/she is listed, the operator may refrain from carrying out processing for marketing purposes.

Once a user has subscribed to the "Do Not Call" register:

- the consent given prior to the subscription is annulled and all data controllers to which her/his telephone numbers are communicated are prevented from using them for marketing purposes; and
- the communication to third parties, the transfer and the spread of her/his personal data for advertising, sale and commercial purposes not related to the business (products and services) offered by the data controller, are forbidden.

By contrast, consent given after subscription to the register is valid.

There is no pan-European list including all communication channels, therefore a user willing to stop unsolicited ads should register on her/his domestic "Do Not Call" register and also on each EU Member State register.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

There is no pan-European list including all communication channels, therefore a user wishing to stop unsolicited ads should register on her/his domestic "Do Not Call" register and also on each EU Member State register.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Italian DPA is active in such enforcement and in case of breaches of marketing restrictions, issues decisions imposing sanctions on data controllers or processor involved in the unlawful processing. Furthermore, the Italian DPA monitors the lawfulness of profiling activities.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

In order to sell marketing lists to third parties, the controller shall provide the data subjects with a privacy statement including the categories of recipients of their personal data, and obtain a separate and specific consent to such communication from the data subject.

A business that purchases marketing lists shall provide the data subjects with a privacy statement including, among other elements, the source of their personal data (i.e. the first data controller).

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Any breach of marketing restrictions is subject to sanctions up to €20 million or up to 4% of worldwide turnover. Furthermore, pursuant to Article 167 of the Privacy Code, if personal data were sold for gain to the data controller or others without consent and the data processing harms the data subject, the data controller shall be punished by imprisonment for six months to one year and a half.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

According to the Italian DPA binding note on 8 May 2014, upon accessing a website, a "short" privacy statement must be displayed in a clearly visible banner and should refer to an "extended" privacy statement.

The banner must specify:

a) if the website uses profiling cookies; and

b) if the website allows "third-party" cookies (i.e. cookies installed by a different website).

By closing the banner, or using the website, users consent to the use of cookies unless they have disabled them.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Cookies may be distinguished into three groups: technical cookies; analytics; and profiling/tracking cookies. No prior consent is required for the use of technical cookies.

In case of third-parties analytics or profiling cookies, users need to be informed appropriately on the purpose of their use in order to give their valid consent.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The Italian DPA has issued several decisions imposing sanctions in case of breaches in relation to the use of cookies.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Breaches of applicable cookie restrictions may lead to sanctions up to €20 million or up to 4% of worldwide turnover.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area may take place – according to a "layered approach" – if the country ensures an adequate level of protection, or the business has implemented one of the required safeguards, or one of particular conditions specified in the GDPR applies.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country not ensuring an adequate level of protection, businesses must guarantee that there are appropriate safeguards, such as, among others, Standard Contractual Clauses drafted by the EU Commission, the Binding Corporate Rules ("**BCRs**"), or contractual clauses agreed between the data exporter and data importer.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

The appropriate safeguards referred to under question 11.2 above may be provided for, without requiring any specific authorisation from a supervisory authority, except for the BCRs and the other safeguards provided for under Article 46.3 of the GDPR, which are subject to authorisation by the competent supervisory authority, and the timing required to obtain it depends on the case.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The scope of corporate whistle-blower hotlines is not limited to any particular issue. According to the Opinion No. 1/2006 of the WP29, businesses responsible for the whistle-blowing scheme should carefully assess whether it would be appropriate to limit the number of persons entitled to report alleged misconduct, as well as the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Pursuant to Article 2-*undecies*, paragraph 1, let. f) of the Privacy Code, data subjects should not exercise the rights provided by Articles 15 to 22 of the GDPR where the exercise could result in a real and concrete prejudice to the confidentiality of the identity of the whistle-blower who reports, according to Law 179/2017 on whistleblowing, the misconduct he/she has become aware of by performing his/her duties.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considered that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement. Businesses should not encourage anonymous reports.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and will not be disclosed to third parties, such as the incriminated person or to the employee's line management. Whistle-blowers should be informed that their identity would be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken when there is a systematic monitoring of a publicly accessible area on a large scale, such as by using CCTV cameras. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the supervisory authority.

The data subjects must always be informed when they enter a monitored area. The controller can make a "simplified" privacy

statement easily available without charge for the data subjects, indicating who is the controller and the purposes pursued, and referring to an "extended" privacy statement containing all the elements provided for by Article 13 of the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

The Italian DPA has issued various decisions concerning CCTV and their limits (the most relevant is the decision issued on 8 April 2010). Among the most relevant: (i) the controller may use CCTV for the purposes of protection and safety of individuals and property, provided that this does not result in an unjustified interference with the fundamental rights and freedoms of the data subjects; (ii) the installation of a CCTV system must comply not only with the legislation on personal data protection, but also with the other national applicable laws (e.g., those regulating the use of remotely controlled devices for employee monitoring).

The other limits on the use of CCTV do not differ from those provided for by the GDPR which are applicable to the processing of personal data through other means.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring shall always be respectful of their fundamental rights, not only with regard to privacy, but also to personal dignity and to freedom of communication and expression. The so-called "**Jobs Act**" amended Article 4 of the Statute of Workers and it provides for a distinction between CCTV (and remotely controlled devices) and other kinds of monitoring.

The former is allowed only if: i) its use is linked to the organisation or production-related needs, or to the safety of the company's assets; and ii) there is a trade union agreement or an authorisation by the local labour authority.

The restrictions under points i) and ii) are not applicable to other tools used by the employees directly to perform their tasks (including smartphones, PCs, etc.) or to the apparatus to record access and presence at the workplace. The data controller must not constantly monitor its employees through these tools for work-related purposes either (which include disciplinary purposes).

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employees must be provided with a proper privacy statement concerning all types of processing, including monitoring carried out as above-described. This shall include: information on the existence, manner, compulsory or non-compulsory nature of the processing; the persons or entities which could process such data; the responsible data processors; and the employees' rights. In the absence of such information to employees, the data cannot be processed.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Trade unions, namely the internal trade union representatives or, in case of undertakings having their seats in different regions, the most representative national trade union associations need to give their agreement for CCTV (and remotely controlled devices). Where there is no agreement, specific authorisation by the local labour authority is required (see question 14.1 above).

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure that they have implemented appropriate technical and organisational measures, which may include: the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems; the ability to restore access to data following a technical or physical incident; and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The controller is responsible for reporting a data breach without undue delay (and in any case, within 72 hours of first becoming aware of the breach) to the relevant supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including: the categories and number of data subjects concerned; the name and contact details of the DPO or other relevant point of contact; and the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subjects, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include: the name and contact details of the DPO (or other relevant point of contact); the likely consequences of the breach; and any measures taken to remedy or mitigate the breach.

The controller is exempt from communicating the breach to the data subject if the risk of harm is remote, it has taken measures to minimise the risk of harm, or the notification requires a disproportionate effort.

15.4 What are the maximum penalties for data security breaches?

Up to €20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative powers	The data protection authority may: order the controller and the processor to provide any information it requires for the performance of its tasks; conduct investigations in the form of data protection audits; carry out review of certificates issued pursuant to the GDPR; notify the controller or processor of alleged infringements of the GDPR; access all personal data and information necessary for the performance of controllers' or processors' tasks; and access the premises where the data are kept, including any data processing equipment.	Not applicable.
Corrective Powers	The data protection authority may: issue warnings or reprimands for non-compliance; order the controller to disclose a personal data breach to the data subject; impose a permanent or temporary ban on processing; withdraw a certification; or impose an administrative fine (as below).	Not applicable.
Authorisation and Advisory Powers	The data protection authority may: advise the controller; or accredit certification bodies and authorise certificates, contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.	Not applicable.
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines, which can be up to €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.	Not applicable.
Non-compliance with a data protection authority	The GDPR provides for administrative fines which will be up to €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year, whichever is higher.	Not applicable.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant supervisory authority to impose a temporary or definitive limitation, including a ban on processing.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Italian DPA regularly issues sanctions or bans on particular data-processing activities when due to their nature, methods or effects, these result in significant prejudice to the data subject. For example, the Italian DPA found the processing carried out by a leading tech company to be unlawful because it was grounded on a general consent provided by users upon signing into the platform on the basis of inadequate information. As a consequence, the Italian DPA banned the company from this processing.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

A data protection authority cannot impose sanctions against a controller established outside its jurisdiction, but can only investigate its activities in the territory of that Member State with the cooperation of the host supervisory authority. In accordance with this principle, the Italian DPA would need to contact the local supervisory authority which is competent in order to seek its cooperation pursuant to Articles 60 to 63 of the GDPR.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

It actually depends on the legal standing (or entitlement) of the law enforcement agencies to request the e-discovery/disclosure of documents, on the type of documents requested, and on the reasons for requesting. In general, it should be taken into account that, other than privacy limitations, strict attorney-privilege limitations also apply in Italy. It should also be noted that e-discovery and disclosure requests are not part of the Italian legal system.

17.2 What guidance has/have the data protection authority(ies) issued?

The Italian DPA has not issued any specific guidance on this topic.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Italian DPA has focused its investigations on data processing in the following sectors: i) data processing carried out by companies and public administrations that manage large databases; ii) data protection measures in credit institutions (especially with reference to data breach reports); and iii) data processing for telemarketing activities. In particular, the Italian DPA has investigated and sanctioned several telecommunications companies for aggressive telemarketing and non-compliance with data protection rules.

18.2 What "hot topics" are currently a focus for the data protection regulator?

The Italian DPA has been issuing decisions to fully implement provisions of the Privacy Code. For example, the Italian DPA has reviewed its general authorisations issued in the past, indicating those that are still valid under the GDPR. Furthermore, it recently issued a list of the kind of processing operations subject to a DPIA pursuant to Article 35 paragraph 4 of the GDPR. Further measures are expected in the following months, such as simplified modalities of compliance with the GDPR for small and medium-sized enterprises.

Carlo Impalà

Morri Rossetti e Associati
Studio Legale e Tributario
Piazza E. Duse no. 2
20122 Milan
Italy

Tel: +39 02 760 7971
Email: carlo.impala@morrirossetti.it
URL: www.morrirossetti.it

As Head of the TMT and Data Protection department, Avv. Carlo Impalà provides legal advice to national and international clients. He deals with corporate and commercial law, and the preparation and implementation of corporate governance and compliance models. He has extensive knowledge of the legislation applicable to the internet, online advertising, data protection, TMT, e-commerce, information technology and outsourcing.

Having graduated in Law, *magna cum laude*, at the University of Palermo, he received an LL.M. in European Legal Studies at the College of Europe in Bruges (Belgium); he also attended a Masters in the field of Digital Business at the Business School of IlSole24Ore.

Carlo has gained a wide range of professional experience at leading international law firms, both in Italy and abroad, and at the Italian Permanent Representation to the EU in Brussels (Belgium).

Carlo is DPO-certified by KHC, and a member of the IAPP (International Association of Privacy Professionals), Federprivacy, Assofintech, and of AmCham's GDPR working group.

He has also been included in the "IP&TMT awards ranking 2019" of the legal directories *Toplegal* and *Legalcommunity*, among the best lawyers in the media and privacy sectors.

MORRI ROSSETTI | STUDIO LEGALE E TRIBUTARIO

Morri Rossetti offers legal and tax advice to national and international clients operating mainly in the telecommunications, media and technology (TMT) sectors, as well as in the digital innovation, e-commerce and online advertising industries.

The TMT and Data Protection department of Morri Rossetti is composed of professionals specialised in several areas of law (in particular, Corporate and Commercial Law, IT and TMT law, Media Law, Privacy and Data Protection, Cybersecurity, Tax Advisory and Tax Compliance) who are able to offer highly innovative and tailor-made solutions, together with a strong sensitivity and ability to understand the business models of such sectors, the opportunities, as well as the legal and tax-critical features of technological evolution.

The integrated and multidisciplinary advice provided by the TMT Team stands out for its high flexibility and efficiency in terms of fees, with an innovative payment system for the services offered – especially to start-ups.

The TMT and Data Protection department has also received important acknowledgments from leading national and international legal directories (e.g. *The Legal 500*, *Toplegal* and *Legalcommunity*) that have recognised the high profile of the assistance and services provided by the Firm to its clients.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com