International Comparative Legal Guides

Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG
Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES
Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

ICLG.com

Expert Chapters

1 **The Rapid Evolution of Data Protection Laws**
Dr. Detlev Gabel & Tim Hickman, White & Case LLP

6 **Privacy, Data Protection, and Cybersecurity: A State-Law Analysis**
Martin M. Zoltick & Jenny L. Colgate, Rothwell Figg

12 **Privacy By Design in Digital Health**
Daniela Fábián Masoch, FABIAN PRIVACY LEGAL GmbH

17 **Initiatives to Boost Data Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune

Q&A Chapters

24 **Albania**
Deloitte Legal Shpk: Ened Topi & Aida Kaloci

33 **Argentina**
Marval O'Farrell Mairal: Gustavo P. Giay & Diego Fernández

42 **Australia**
Nyman Gibson Miralis: Dennis Miralis & Phillip Gibson

54 **Austria**
Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit

65 **Belgium**
LYDIAN: Bastiaan Bruyndonckx & Olivia Santantonio

77 **Brazil**
Pellon de Lima Advogados: Rafael Pellon & Nathalia Santos

86 **China**
King & Wood Mallesons: Susan Ning & Han Wu

97 **Cyprus**
Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas

109 **Czech Republic**
White & Case, s.r.o., advokátní kancelář: Ivo Janda & Anna Stárková

119 **Denmark**
Synch Advokatpartnerselskab: Christine Jans & Heidi Højmark Helveg

131 **France**
Clyde & Co: Benjamin Potier & Pierre Affagard

141 **Germany**
SKW Schwarz Rechtsanwälte: Nikolaus Bertermann

150 **Ghana**
Addison Bright Sloane: Victoria Bright & Justice Oteng

159 **India**
Khaitan & Co LLP: Harsh Walia & Supratim Chakraborty

169 **Indonesia**
SSEK Indonesian Legal Consultants: Denny Rahmansyah & Raoul Aldy Muskitta

178 **Ireland**
Matheson: Anne-Marie Bohan & Chris Bollard

190 **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O'Connor

200 **Israel**
Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Efrat Artzi

211 **Italy**
DDPV Studio Legale: Luciano Vasques & Chiara Sciarra

223 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa

234 **Korea**
D'LIGHT Law Group: Iris Hyejin Hwang & Hye In Lee

244 **Kosovo**
Deloitte Kosova Shpk: Ardian Rexha & Ened Topi

253 **Luxembourg**
NEOVIAQ IP/ICT: Raymond Bindels & Milan Dans

264 **Mexico**
OLIVARES: Abraham Díaz Arceo & Gustavo Alcocer

273 **Nigeria**
Templars: Emmanuel Gbahabo & Oghomwen Akpaibor

286 **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten & Emily M. Weitzenboeck

298 **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan

306 **Poland**
Leśniewski Borkiewicz & Partners: Grzegorz Leśniewski, Mateusz Borkiewicz & Jacek Cieśliński

317 **Russia**
Semenov&Pevzner: Ekaterina Smirnova

326 **Senegal**
LPS L@w: Léon Patrice Sarr

Q&A Chapters Continued

335 **Singapore**
Drew & Napier LLC: Lim Chong Kin

349 **South Africa**
PPM Attorneys: Delphine Daversin & Melody Musoni

359 **Spain**
Elzaburu S.L.P.: Ruth Benito Martín & Alberto López Cazalilla

370 **Switzerland**
Homburger AG: Dr. Gregor Bühler, Luca Dal Molin & Dr. Kirsten Schmidt

379 **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Sam Huang

389 **Thailand**
Chandler MHM Limited: Pranat Laohapairoj
Mori Hamada & Matsumoto: Atsushi Okada

397 **Turkey**
SEOR Law Firm: Okan Or & Basak Feyzioglu

407 **United Kingdom**
White & Case LLP: Tim Hickman & Matthias Goetz

417 **USA**
White & Case LLP: Steven Chabinsky & F. Paul Pittman

Italy

Luciano Vasques

Chiara Sciarra

DDPV Studio Legale

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal national data protection legislation in Italy is Legislative Decree no. 196 of 30 June 2003 (the Italian Data Protection Code – "**IDPC**"), as amended by Legislative Decree no. 101 of 10 August 2018, which was enacted in order to make the Italian data protection laws compliant with EU Regulation 2016/679 (the General Data Protection Regulation – "**GDPR**"). The IDPC implemented the Privacy and Electronic Communications Directive (EU Directive 85/2002).

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

The only general legislation about data protection in Italy is the GDPR and the IDPC.

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

Several pieces of national legislation have an impact on privacy law: Law 300/1970 limits the use of CCTV systems in work spaces; Legislative Decree no. 70/2003 (the e-Commerce Law) establishes mandatory rules directly applicable to e-commerce; Legislative Decree no. 206/2005 (the Consumer Code) provides for specific rules regarding consumer protection; Legislative Decree no. 81/2008 provides for specific rules regarding both health and safety in the workplace; Presidential Decree no. 178/2010 (Public Register of Objections) and its integrative Decree no. 149/2018 establish the opt-out regime for marketing purposes through electronic and mailing means; Law 179/2017 limits access to personal data in case of whistle-blowing proceedings; and Law 5/2018 regulates telemarketing calls.

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

In Italy, the authority responsible for data protection is the Italian Privacy Authority (*Autorità per la Protezione dei Dati Personali* – "**IPA**"), which is based in Rome (contact information: Piazza Venezia no. 11 – 00187; +39 06 696 771; protocollo@gpdp.it; https://www.garanteprivacy.it).

The IPA is assisted in its investigations and inspections by a specialised privacy division of the Italian Finance Police (*Guardia di Finanza*).

2 Definitions

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

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on 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**" means 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**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" means 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.
- "**Data Breach**" means 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.
- "**Direct Personal Data**" means data that allow for the direct identification of a physical person – such as personal data (for example, name and surname), images, etc.
- "**Indirect Personal Data**" means data that allow for the indirect identification of a physical person, such as an identification number (for example, a tax code, IP address or licence plate number).

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 IDPC applies to businesses that are established in Italy, and to the processing of personal data (either as a controller or processor, and regardless of whether or not the processing takes place in Italy) in the context of that establishment. A business that is not established in any Member State, but is subject to the laws of Italy by virtue of public international law, is also subject to the IDPC (and, in general, to the GDPR).

The IDPC applies to businesses outside Italy if they (either as controller or processor) process the personal data of Italian residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to Italian residents (see IPA dec. 28 June 2019, *Facebook – Cambridge Analytica*); or (ii) the monitoring of Italian residents' behaviour (to the extent that such behaviour takes place in Italy).

The IDPC applies to businesses established outside the EU if they process personal data in Italy.

4 Key Principles

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

- **Transparency**
  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- **Lawful basis for processing**
  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., 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) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU and/or IDPC, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects).
  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected 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. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Retention**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data security**
  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

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 in respect of the data subject's personal data: (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) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria in order to determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  Additionally, the data subject may request a copy of the personal data being processed.
  The IDPC provides some exceptions to the EU principles described above.

In particular, the right of access to data may not be exercised, or can be limited, if it may effectively be detrimental to any of the following:

i) The interests safeguarded by anti-money laundering provisions.

ii) The interests safeguarded by the provisions aimed at supporting victims of extortion.

iii) The activities of Parliamentary enquiry committees set up pursuant to Article 82 of the Italian Constitution.

iv) The activities carried out by a public body other than a profit-seeking organisation as expressly provided for by a law for purposes relating exclusively to monetary policies, the system of payments, oversight over credit and financial brokers and markets, and the protection of market stability.

v) Restrictions based on judicial proceedings; in particular, the IDPC provides further restrictions related to the processing of personal data that is carried out on judicial grounds in connection with proceedings before civil, criminal and administrative courts, as well as proceedings before self-governance bodies of special judicial authorities (such as the *Consiglio Superiore della Magistratura*) or before the Ministry of Justice.
The IDPC provides that the processing of this kind of personal data must be regulated by the special rules applicable to the said proceedings. For this purpose, processing activities on judicial grounds do not include the standard management and administrative activities of the staff, equipment or facilities concerned, provided that this is not prejudicial to the confidentiality of instruments that are related directly to the handling of judicial proceedings.

vi) Confidentiality regarding the identity of a whistle-blower pursuant to Italian Whistle-blowing Law (Law 179 of 30 November 2017).

vii) Protected interests regarding taxation and the performance of activities aimed at preventing and countering tax evasion.
In all these cases (except for point iii), the rights as per the said paragraph shall be exercised in accordance with the laws or regulations applying to the individual sectors. Exercise of the rights in question may be delayed, restricted or ruled out, in which case the data subject shall be informed of the relevant reasons without delay, except where that may be prejudicial to the purpose of the restriction.

viii) Restrictions related to rights concerning deceased persons.
Although the GDPR excludes from its application the personal data of deceased persons, it allows Member States to provide for rules concerning the processing of such data.
The IDPC grants confidentiality rights to the personal data of deceased persons. These rights can be exercised by those who have a legitimate personal interest in the confidentiality of such data (for example, they relate to a member of his/her family) or by an authorised representative of the deceased person. As regards the request for access to health documentation, the IPA denies free access to health-related data of a deceased person (see IPA press release of 15 April 2019).

- **Right to rectification of errors**
Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**
Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the data subject withdraws his/her 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 processed unlawfully; or (v) erasure is necessary for compliance with the GDPR and/or IDPC.

- **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 basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or require the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**
Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

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

- **Right to withdraw consent**
A data subject has the right to withdraw his/her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**
A data subject has and must have the right to deny or withdraw his/her consent to the use of his/her contacts for marketing purposes and profiling. The processor has to ensure that the processing is organised in such a way that this right is effective.
In Italy, an opt-out register (*Registro Pubblico delle Opposizioni* – "**RPO**") has been set up. The RPO is a "Do Not Call" register that allows individuals whose telephone number is listed in a public telephone directory to opt out of receiving unsolicited telemarketing calls.

- **Right to complain to the relevant data protection authority (IPA)**
Data subjects have the right to lodge complaints with the IPA concerning the processing of their personal data, if the data subjects live in Italy or the alleged infringement occurred in Italy. A personal data breach can be notified to the IPA at protocollo@pec.gpdp.it by certified email, at protocollo@gpdp.it by ordinary email, or by registered letter to the IPA address (see question 1.4.).
A data breach notification template has been made available by the IPA on its website.

- **Right to basic information**
  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

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 of the processing of "sensitive data" to the IPA (provided before the implementation of the GDPR and of the IDPC) has been erased by Article 22.8 of the IDPC and no longer applies.

In the event that a personal data breach occurs, the controller and or the processor shall notify the IPA of the breach (see section 15).

In certain circumstances, when a controller, in the completion of a data protection impact assessment ("**DPIA**") (in compliance with the criteria set forth by the Article 29 Working Party ("**WP29**") and with the Guidelines on Data Protection Impact Assessments – WP 248) ascertains a "high risk" of processing, where the assessment indicates that the risk cannot be mitigated, the controller must consult the IPA. The IPA has published a list of processing operations subject to the requirements of the DPIA.

There is a duty to communicate to the IPA (pursuant to Article 119 *bis* of the IDPC) if an entity needs to reuse personal data for scientific research and/or statistical purposes and it is practically impossible to duly inform each data subject without jeopardising the achievement of the research.

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)?

See question 6.1.

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

See question 6.1.

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)?

See question 6.1.

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)?

See question 6.1.

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

See question 6.1.

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

See question 6.1.

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

This is not applicable; see question 6.1.

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

See question 6.1.

6.10 Can the registration/notification be completed online?

See question 6.1.

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

The processing register for notification is accessible on the IPA website (updated before the implementation of the GDPR).

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

This is not applicable; see question 6.1.

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.

According to Article 37 of the GDPR, the controller and the processor shall designate a Data Protection Officer ("**DPO**") in any case where: (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

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

In the event of failure to appoint the DPO in cases of obligation, the IPA can charge a fine of up to €10 million; for undertakings,

the IPA can charge a fine of up to 2% of the total annual global turnover of the previous year, if this percentage is higher than €10 million.

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?

The DPO must be protected from disciplinary measures, or other employment consequences, in respect of his/her role as a DPO. Although no specific rules are provided, in practice a DPO must have the independence required by the GDPR and by the IDPC. This independence is not compatible with any potential disciplinary measures, or other employment consequences related to his/her role as DPO (except if the disciplinary measures to which the DPO is subject are adopted because the DPO has not appropriately performed his/her activity, to the detriment of the interests of the data owners).

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

Different companies can appoint the same person responsible for the protection of personal data (for example, a DPO for different companies belonging to the same group), provided that the DPO is easily contactable from each company assisted. In addition, the DPO must be able to communicate effectively with each company, and must have effective communication with the IPA with regard to all the companies assisted. Also, a legal person can be appointed as DPO.

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

Under Italian law, the DPO is not required to have specific formal attestations or registration in specific registers. However, he/she must have an in-depth knowledge of privacy legislation and practices, as well as the administrative rules and procedures which characterise the specific sector where the controller and/or the processor operate.

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

A DPO should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the DPO, which include: (i) informing the controller, processor and their relevant employees who process data about their obligations under the GDPR; (ii) monitoring compliance with the GDPR, the IDPC and other applicable internal policies in relation to the processing of personal data, including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the IPA and acting as the authority's primary contact point for 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)?

Yes, the appointment of the DPO must be communicated to the IPA. The communication can be done by filling in the data of the DPO and of the controller/processor on an electronic form available through a page on the IPA's website (https://servizi.gpdp.it/comunicazionerpd/s/compilazione-comunicazione).

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

The DPO does not necessarily need to be named in a public-facing privacy notice. As a matter of good practice, the WP29 (now the European Data Protection Board – "**EDPB**") recommended, in its 2017 guidance on DPOs, that both the data protection authority and employees should be notified of the name and contact details of the DPO.

It is good practice for the DPO's contact details to be made public through publication on the controller/processor's official website, on a specific page displaying the privacy information policy notice.

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?

The relationship between the controller and the processor must be regulated by a written agreement.

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 processor must be appointed under a binding agreement in writing. The Agreement has to regulate the subject matter for processing, the duration of processing, the nature and purpose of processing, the types of personal data and categories of data subjects. In particular, the contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or applicable Italian law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

The Agreement has to regulate how the personal data are managed in the event that the Agreement is terminated (in compliance with GDPR and IDPC rules).

The controller may subcontract part of its functions to another controller or appoint a co-manager with the written authorisation of the controller only.

A processor can be an entity established in the EU or a non-EU entity with a legal representative established in Italy.

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 sending of electronic direct marketing is allowed when the recipient has given his/her consent. In particular, data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

The use of automated calling or email, facsimile, MMS or SMS for the purposes of direct marketing or sending advertising materials, or for carrying out market surveys, is allowed only with the contracting party's or user's prior consent.

The IPA requires appropriate mechanisms for contracting parties (for example, the client of a phone services company) to give their appropriate and fully informed consent to inclusion in directories, as well as to the use of their data for the purposes of sending advertising materials, direct selling, marketing surveys or marketing communications.

The use of automated calling or communications systems without human intervention for the purposes of direct marketing or sending advertising materials, or for carrying out market surveys or interactive business communication, shall only be allowed with the contracting party's or user's specific consent for this kind of communication.

This principle also applies to electronic communications performed by email, facsimile, MMS or SMS-type messages or other means for the purposes referred to therein, including if these contacts are available on the web (see IPA dec. no. 378, 21 September 2017; and IPA dec. no. 327, 20 July 2017).

By way of derogation, and concerning only marketing communication carried out by email (this exception does not apply to marketing communication by telephone calling, MMS or SMS), where a data controller uses, for direct marketing of his/her own products or services, electronic contact details for electronic email supplied by a data subject in the context of the sale of a product or service, said data controller can avoid requesting the prior consent of the data subject on condition that the services are similar to those that have been the subject of the sale, and that the data subject, after being adequately informed, does not object to subsequent communications. In any case, for marketing communications concerning different services or services provided by third parties, prior consent of the data subject is always necessary.

9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

No, these provisions are not applicable in a business-to-business context. Legal persons cannot rely on the GDPR safeguards and they may only avail themselves of ordinary means of protection.

An employee's business email address and telephone number are considered personal contact details of the employee, and are protected by the GDPR and the IDPC restrictions applicable to business-to-consumer marketing rules.

9.3 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.).

Processing by telephone (on a fixed or mobile telephone number lawfully available in public-domain directories or in public-domain sources) for the purposes of sending advertising materials, direct selling, marketing surveys or marketing communications (except marketing activities done with the use of automated calling or communications systems without human intervention) shall be allowed in respect of any entities that have not exercised their right to no longer receive unsolicited direct marketing calls and postal mail.

A natural person whose telephone number is listed in the public telephone directories can contact the RPO (a foundation authorised by the Italian Ministry of Economic Development) in order to request to stop receiving unsolicited calls and postal mail from any direct marketing operator.

The RPO can be contacted via an e-form on its website (http://www.registrodelleopposizioni.it) or by email, phone call or certified mail. The RPO's service is free of charge.

A marketing operator can have periodic access to the RPO's database and access the data and/or update the data lists of telephone numbers that cannot be contacted for marketing purposes.

Subscription to the "Do Not Call" register determines the annulment of the data subjects' consent given for using his/her telephone number and postal address for marketing purposes (except with regard to the use for marketing purposes of publicly available information). By contrast, consent given after subscription to the register is valid.

Subscription to the "Do Not Call" register only prevents the use of the numbers contained in the telephone directories for promotional calls, and does not forbid the use of the data (fixed or mobile number, email) legitimately collected and subsequently authorised to be used for marketing purposes on the basis of a legitimate consent otherwise given to third parties on the basis of contractual agreements; for example, on the occasion of the purchase of goods or services, or on the occasion of enrolment in loyalty programmes, participation in prize competitions, etc.

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

Theoretically, yes, if the marketing activities concern Italian residents (Italian telephone numbers). In reality, it is more difficult for the IPA to perform any enforcement against non-Italian entities, especially if they are based in non-EU countries.

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

The IPA is in charge of the enforcement of any breaches of marketing restrictions.

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

The transfer of personal data by the controller is admissible if it has: (i) informed the data subject about the possibility of transferring his/her personal data; or (ii) acquired specific consent to transfer data to third parties. Consent to transfer data to third parties must be obtained by means of separate specific wording (it is not enough to have the consensus given for receiving newsletters or profiling from third parties).

The consent formula must indicate the categories of subjects to whom the data will be transferred (provided that the data subject has expressed consent in this regard).

In addition, the purchaser of the data, before processing them, must communicate its privacy information to the data subject so that he/she can also exercise his/her rights in respect of the entity which purchases the data.

If the entity to whom the personal data may be transferred is indicated individually (therefore not referring to the categories) and the information of the transferring company presents all the elements required by Article 13 of the GDPR (with reference to the treatment that will be carried out by the entity which could purchase the data), it is not necessary for the entity which acquires the data, following the transfer, to release further information to the interested parties (the purchaser has to provide appropriate contact details for the exercise of the user's rights only).

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

Any breach of marketing restrictions is subject to sanctions of 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 to 18 months.

The most interesting cases are the following:

1) On 11 December 2019, the IPA imposed two fines on Eni Gas and Luce, totalling €11.5 million, concerning, respectively, the unlawful processing of personal data in the context of promotional activities, and the activation of unsolicited contracts.
2) On 23 January 2020, the IPA fined Runwhip €80,000 for not having provided the requested information related to the contents of its databases. The proceeding concerned a data subject's claim for unsolicited promotional marketing calls by Sky Italia S.p.A. The data subject exercised his right to deny his consent to the use of his contacts for marketing purposes, and he also exercised the right to access his personal data held by Sky, but Sky declared that it had acquired the data from Runwhip. In conclusion, the complainant had repeatedly asked Runwhip to grant him access to his personal data, but without receiving any response.

10 Cookies

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

The IDPC implements Article 5 of the EU ePrivacy Directive, pursuant to which the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2020.

The IPA's binding note of 8 May 2014 provides that when a user accesses a website, a "short" privacy information notice must be shown in a visible banner, referring to an "extended" privacy statement. The banner must inform the user about the use of cookies and it must specify if the website hosts cookies of third parties. The banner mechanism provides that if the user closes the banner or continues to browse the website without disabling the cookies, this means that the user accepts the use of cookies.

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

The IPA distinguishes three groups of cookies: (i) technical cookies (for the use of this kind of cookies, no prior consent is required); (ii) analytics cookies (prior informed consent is required); and (iii) profiling cookies, which are used to create user profiles in order to send targeted advertising messages (prior informed consent is required).

In the case of both third-party analytics and the profiling of cookie users, prior informed consent is required.

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

The IPA 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?

Violations of cookie restrictions may lead to sanctions of 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.

According to the GDPR, data transfer inside the European Economic Area ("**EEA**") is permitted, while data transfers to jurisdictions outside the EU and the EEA is not always allowed. A data transfer abroad can only take place to a whitelisted country and it must respect the following rules: (i) it must use Standard Contractual Clauses and Model Contracts; (ii) it must follow binding corporate rules; (iii) it must have an approved certification; and (iv) it must have an approved code of conduct.

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 other than an Adequate Jurisdiction, businesses must guarantee the application

of appropriate safeguards to the data transfer; for example, Binding Corporate Rules ("**BCRs**"), Standard Contractual Clauses (drafted by the EU Commission) and Model Contracts. BCRs will always need approval from the IPA.

The Standard Contractual Clauses drafted by the EU Commission are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer, provided that they conform to the protections outlined in the GDPR, and they have prior approval by the IPA.

Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR, and the relevant complaints procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

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.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism, as set out above, for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

The safeguards for data transfers abroad outlined in question 11.2 generally do not need any authorisation from the supervisory authority (e.g., for the use of Model Contracts). There is an exception for BCRs, which must be approved by the supervisory authority. In this case, the proceeding, if all the required information is available, has a maximum duration of 18 months.

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.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel, and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. In the Opinion, it is recommended that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme, and whether it might be appropriate to limit the number of persons who may be reported through the scheme; in particular, in the light of the seriousness of the alleged offences reported.

There are no particular restrictions to the scope of corporate whistle-blower hotlines. The businesses responsible for the whistle-blowing procedure should assess whether it is necessary to set limits regarding, for example, the number of persons who can access to the scheme, on the side of both the reporting and reported party.

The IDPC provides that the rights referred to in Articles 15 to 22 of the Regulation may not be exercised if the exercise of those rights may prove detrimental to the confidentiality regarding the identity of whistle-blowers pursuant to Law 179 of 30 November 2017.

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 under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should *not* encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

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 establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all stages of the process and, in particular, will not be disclosed to third parties, such as the incriminated person or the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted under 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 with assistance from the DPO when there is systematic monitoring of a publicly accessible area on a large scale. 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 IPA.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing,

a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and, where applicable, the contact details of the DPO.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation, and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

If a company is using instruments aimed at systematic monitoring of a publicly accessible area on a large scale (e.g., CCTV), it is necessary:

i) to inform the data subjects that they are entering a monitored area by providing a privacy statement indicating the controller; and
ii) to undertake a DPIA in order to assess the level of risk to the fundamental rights of freedom. If a high risk emerges from the DPIA, the controller must consult the IPA.

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

The IPA has provided some limits on the purposes for which CCTV data may be used. In particular, the use of CCTV cameras must comply with data protection legislation and with the other national principles and laws. Furthermore, CCTV systems can be used exclusively for organisational and production needs, for the safety of the work, without prejudice to the data subjects' fundamental rights.

14 Employee Monitoring

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

Employee monitoring systems must be respectful of fundamental rights such as freedom, privacy and dignity. With regard to employee monitoring, the main provision is represented by Article 4 of Law 300 of 1970 ("**Statute of Workers**"), which distinguishes CCTV and remotely controlled devices from other kinds of employee monitoring. In particular, CCTV systems and other instruments from which the possibility of remote control of workers' activity derives can be used exclusively for organisational and production needs, for the safety of the work and for the protection of company assets, and it is necessary that the use of CCTV is specifically authorised by a trade union agreement or by the National Labour Inspectorate ("**NLI**").

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

Companies that use monitoring systems must provide their employees with a privacy statement giving all the information about the monitoring systems adopted, such as the fact that an area is monitored, the person who could process the data, the employees' rights and the purpose of monitoring. Providing this information is compulsory, otherwise the data cannot be processed.

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

Systems for remote monitoring of workers' activity can be installed subject to the collective agreement stipulated between the employees and the local trade union association. Alternatively, in the case of undertakings with production units located in several Italian provinces, such agreement may be stipulated by the comparatively more representative trade unions at the national level.

In the absence of agreement with the competent trade union association, the above-mentioned instruments may be installed subject to authorisation from the territorial office of the NLI or, alternatively, in the case of undertakings with production units located in the areas of most territorial offices, from the headquarters of the NLI.

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.)?

Yes. 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 they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an 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 personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the IPA, 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 relevant point of contact, 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 subject, 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 point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

On 23 January 2020, the IPA fined Verona Hospital €30,000 for processing personal data in breach of Article 5 letter f. of the GDPR. The hospital did not ensure the security of the personal data; in particular, the IPA outlined unauthorised accesses to the clinical records of 16 patients (IPA dec. no. 18 2020).

On 23 January 2020, the IPA imposed a €30,000 fine on a university in Rome (La Sapienza) for having disclosed personal data processed through the university platform used to collect whistle-blower reports. In particular, the university made two whistle-blowers' common personal data (name and email address) available on search engines (IPA dec. no. 17 2020).

16 Enforcement and Sanctions

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

Investigatory/Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The IPA has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out review on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks, and to access the premises of the data including any data processing equipment.	If the IPA ascertains facts that represent criminal offences, it must communicate those facts to the public prosecutor (*Procura della Repubblica*) without delay. The IDPC provides several criminal sanctions for heavy infringements of the IDPC provisions.
Corrective Powers	The IPA has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification, and to impose an administrative fine (as below).	N/A
Authorisation and Advisory Powers	The IPA has a wide range of powers to advise the controller, accredit certification bodies and authorise certificates, contractual clauses, administrative arrangements and binding corporate rules, as outlined in the GDPR.	N/A
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 proceeding financial year.	N/A
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 proceeding financial year, whichever is higher.	N/A

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 data protection 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 IPA generally issues proceedings against the data processing that may affect rights of the data subjects. The IPA decides the amount of the fine, taking into consideration the gravity of

the infringement and the annual turnover if an undertaking is involved. If a data subject is involved, the IPA applies proportional criteria and a graduated approach.

The IPA imposed a roughly €2 million fine on a call centre operator (Vincall) for violation of several IDPC rules in conducting a telemarketing campaign on behalf of an energy company (Edison) (IPA dec. no. 95 2019).

The IPA imposed a €50,000 fine on a political party for not having adopted appropriate measures and procedures to avoid a data breach (IPA dec. no. 83 2019).

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

The IPA can only carry out investigations in another Member State with the cooperation of the supervisory host. The IPA has imposed a fine on a company incorporated in Ireland for an alleged infringement which also occurred in the Italian territory (*Facebook – Cambridge Analytica* case, IPA dec. no. 134 2019).

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 depends on the legal standing (or entitlement) of the law enforcement agencies to request the discovery/disclosure of documents, on the type of documents requested, and on the reasons for the request. 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 IPA has not provided any guidance on this matter.

18 Trends and Developments

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

The IPA fined TIM S.p.A. ("**TIM**", a telecommunications company) €27.8 million (0.2% of TIM's total annual turnover) for several unlawful marketing data processing practices (contact with consumers which denied their consent to be contacted for marketing, invalid methods to collect users' consent, and lack of accountability) (IPA dec. no. 7 2020).

The IPA imposed a €1 million fine in the *Facebook – Cambridge Analytica* case. The IPA ascertained that 57 Italians had downloaded the "thisisyourdigitallife" app via Facebook's login function; thanks to the sharing of data relating to "friends" enabled by that function, the app had subsequently acquired data relating to an additional 214,077 Italian data owners who had not downloaded the app in question, had not been informed of the sharing of their data and had not given their consent to such sharing, in breach of IDPC provisions (IPA dec. no. 134 2019).

On 22 July 2019, the IPA issued a judgment involving the so-called "right to be forgotten". The case involved a physical person who requested Google to remove a link to online content (an article in a newspaper – the "**Article**") about him concerning a criminal proceeding which had occurred approximately a decade earlier, as the Article had not been updated (in the meantime, the criminal proceeding had terminated with an acquittal of the physical person involved). Google rejected the request of the physical person to remove the URL of the Article. The physical person submitted a complaint to the IPA, and the IPA ordered Google to remove the URL of the Article.

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

One hot topic is data donation and the personal data of deceased persons in the context of privacy principles.

Another issue of current interest is the debate about simplified modalities of compliance with the GDPR for small and medium-sized enterprises and non-profit organisations in Italy.

Luciano Vasques concentrates on antitrust, consumer protection, privacy, energy and other regulatory matters in Italy and the European Union, and on corporate law (bankruptcy proceedings).
As an officer of and counsel to the Italian Antitrust Authority, Mr. Vasques was involved in proceedings in the Italian manufacturing, oil, energy, gas, water distribution, waste disposal (domestic and industrial waste) and public utilities sectors.
He advises clients on Italian and EU antitrust matters, such as investigations by the Italian Antitrust Authority and the EU Commission concerning alleged agreements against competition, concerted practices, abuse of dominant position, antitrust litigation cases (antitrust private enforcement), as well as complex antitrust issues arising from merger and acquisition transactions (Italian, EU and multijurisdictional filings).
Mr. Vasques also assists his clients on consumer protection, unfair competition, multi-level marketing business, state aid issues, telecommunications, electricity and gas regulations, and also has consolidated expertise in transactions concerning the creation and sale of renewable power plants.
Mr. Vasques has written widely on antitrust, unfair competition and corporate law for leading Italian and international periodicals, and is the author of a book on the application of antitrust principles relating to Italian public utilities.

DDPV Studio Legale
Piazzale delle Belle Arti no. 2
00196 Rome
Italy

Tel: +39 06 3600 1188
Email: l.vasques@ddpvlex.com
URL: www.ddpvlex.com

Chiara Sciarra is a trainee lawyer at DDPV Studio Legale in Rome. She mainly works in the antitrust, consumer protection and privacy sectors, assisting clients and drafting defensive submissions before the civil and administrative courts. She also participates, as a trainee, in compliance procedures before the Italian Antitrust Authority.
Ms. Sciarra graduated in 2019 from Luiss Guido Carli University in Rome with a Master's thesis on "gun-jumping" and EU merger control. She attended the Erasmus Programme at Radboud University in Nijmegen (Netherlands), focusing on Copyright Law and Competition Law.

DDPV Studio Legale
Piazzale delle Belle Arti no. 2
00196 Rome
Italy

Tel: +39 06 3600 1188
Email: info@ddpvlex.com
URL: www.ddpvlex.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Fintech
Foreign Direct Investment Regimes
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
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group