

PERSONAL DATA PROTECTION – RECENT DEVELOPMENTS IN ITALY

Italy's data protection authority (the "**Italian DPA**") has now reviewed for compliance with the GDPR the various **codes of conduct and professional practice** that applied, and the general authorisations that had been issued, under the previous legislation. **The rules thus approved will be binding**, and their breach will be punished by the imposition of the toughest available administrative penalty (a fine of up to €20 million or 4% of global annual revenues).

Other key developments have occurred since the entry into force of Legislative Decree 101/2018 (the "**GDPR Decree**"), which last September brought Italy's domestic law into line with the GDPR: the Italian DPA provided a list of categories of processing operations that are subject to the requirement for a data protection **impact assessment** and signed a **memorandum of understanding** with the Rome prosecution service, so that investigations into personal data protection offences may be carried out more quickly and effectively.

THE REVISED CODES OF CONDUCT

Under five decisions issued over November and December 2018,¹ the Italian DPA had reviewed the compliance with the General Data Protection Regulation, No. 2016/679 (the "**GDPR**") of the terms of various pre-existing codes of conduct and professional practice. These related to the processing of personal data in the conduct of **journalism, for the purposes of historical, statistical or scientific research**, and in the **preparation of a case in a lawsuit**, and had formed Schedules A.1, A.2, A.3, A.4 and A.6 to Legislative Decree 196/2003 (the "**Data Protection Code**").

These codes of conduct and professional practice have been revised to make them consistent with the GDPR, and renamed "rules of professional practice" pursuant to article 20(4) of the GDPR Decree. They have been passed to the Ministry of Justice in order that it may issue a decree for their inclusion in Schedule A to the Data Protection Code, as amended by the GDPR Decree. The rules of professional practice related to the processing of personal data in the conduct of journalism and for the purposes of

Key issues

- The Italian DPA has reviewed the codes of professional practice and the existing general authorisations for compliance with the GDPR
- Breach of the rules of professional practice or the general authorisation may result in the imposition of the toughest available administrative penalty
- The rules of professional practice that allowed disclosure to data subjects to be deferred where the data had come directly from those subjects have been eliminated
- The Italian DPA has set out specific rules for processing data during the pre-hiring phase
- The Italian DPA has identified the kinds of processing operations that require a DPIA
- New privacy litigation of the so-called Foodora bicycle couriers
- Quicker and more effective procedures for investigating breaches of the law connected with criminal offences

¹ Decision No. 491 of 29 November 2018, and Decision Nos. 512 513 514 and 515 of 19 December 2018, available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069732>.

statistical or scientific research were published in Italy's Official Gazette No. 3 of 4 January 2019 and No. 11 of 14 January 2019, respectively, while those relating to preparation of a case in a lawsuit were published on No. 12 of 15 January 2019. ²

Starting from publication in the Italy's Official Gazette³, **compliance with the rules of professional practice constitutes an essential condition for processing of personal data** within these fields to be considered to have been carried out lawfully and properly (article 2-*quater*(4) of the Data Protection Code, as amended). Their breach shall be punishable by an **administrative fine** of up to €20 million, or, for enterprises, up to 4% of total global annual revenues in the previous financial year, where this is higher (article 166(2) of the Data Protection Code, as amended).

With respect to the content of the rules of professional practice, the Italian DPA made changes both formal and substantive:

From a formal standpoint, the Italian DPA:	From a substantive standpoint, the Italian DPA:
Revised the references to laws and regulations, and the language used, to make them consistent with the changed regulatory environment put in place by the GDPR and the revised Data Protection Code. Specifically, the Regulator has made merely formal, rather than substantive, changes to the existing Schedules A.1 (Journalism), A.2 (Historical research), and A.6 (Investigations in preparation of a legal case).	Eliminated the provisions that enabled the controller to provide deferred and/or simplified disclosure to data subjects, where the personal data had been obtained directly from the data subject. This reflected article 13 of the GDPR, which does not provide for any form of exception to the notice obligations, or simplifications of the disclosures that have to be made.
Eliminated the preambles to all the rules, reflecting the fact that article 20 of the GDPR Decree required it only to consider the effective provisions contained in the rules.	Eliminated the provisions that had obliged data controllers that were going to obtain personal data from third parties to give the Italian DPA prior notice of how they intended to publicly announce the disclosures.
	Eliminated the provisions that had governed the conditions upon which processing was lawful (now laid down in articles 6 and 7 of the GDPR).
	Eliminated the provisions that had governed transfers of personal data to third countries (now dealt with in articles 44 et seq. of the GDPR).

The remaining two pre-existing Schedules, **A.5** and **A.7**, related to **information systems** managed by non-public entities in connection with consumer credit, and payment reliability and punctuality, and data processing for the purposes of **commercial information**. Pursuant to article 20.1, these will **remain in force until 19 September 2019**, provided that:

- By 19 March 2019, the associations and other bodies that represent the kinds of companies that are data controllers and data processors for these kinds of activities submit codes of conduct compliant with article 40(2) of the GDPR to the Italian DPA for its approval; and
- Such approval is forthcoming within the six months thereafter.

² As the Regulator made clear in [its press release of 28 December 2018](#), article 20 of the GDPR does not require a public consultation at this stage. Nonetheless, the legislation requires **public consultation for rules of professional practice adopted hereafter, or in connection with any subsequent amendments to the rules now adopted**. It remains open to the Italian DPA subsequently to revise those terms, or to adopt new sets of rules of professional practice, applying the procedure under article 2-*quater* of the revised Data Protection Code, which requires a public consultation process of at least 60 days.

³ At that time, the old codes of conduct and professional practice set forth in Schedules A.1 A.2 A.3 A.4 and A.6 to the Data Protection Code ceased to be in force, pursuant to article 20(3) of the GDPR Decree.

Failure to comply with either of those deadlines will mean the terms of those Schedules shall cease to be effective from the expiry of any such term.

Aside from the differences in the procedures that have been established for those two sets of Schedules, there are also **differences of structure and function** between rules of professional practice, and codes of conduct under article 40(2) of the GDPR:

	Rules of professional practice	Codes of conduct
Differences of structure	<p>Rules of professional practice may only be introduced in those sectors specifically identified by the GDPR and the Data Protection Code (under article 2-<i>quater</i> of the Data Protection Code).</p> <p>This means in connection with processing under articles 6(1)(c), (e), and 9(4), and Chapter IX of the GDPR, i.e.: in the context of employment, and the processing of personal data from archives, registers, lists, instruments and documents kept by public registries, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (under articles 61, 102 106 and 111 of the Data Protection Code).</p>	<p>Codes of conduct may be introduced in any sector.</p> <p>Merely by way of example, article 40(2) GDPR lists eleven fields in which the preparation of codes of conduct is being encouraged at a European level.</p>
Differences of function	<p>When approved, rules of professional practice become binding rules, effective as if they had been authored by the Italian DPA. Compliance with such rules is essential for processing in those contexts to be lawful and proper.</p> <p>Their breach will be punished by the imposition of the toughest available administrative penalty (a fine of up to €20 million or 4% of global annual revenues).</p>	<p>Under the European legislation codes of conduct are merely forms of self-regulation by associations and other bodies representing classes of data controllers and processors within particular sectors.</p> <p>The associations and bodies remain the effective authors of such codes, approval by the Italian DPA is a secondary matter, and failure to comply with their terms does not mean the processing is unlawful.</p>

GENERAL AUTHORISATIONS

In a decision of 13 December 2018,⁴ the Italian DPA (i) identified the provisions among the authorisations set out in the general authorisations (adopted pursuant to articles 26 and 40 of the Data Protection Code⁵, now abolished) that were compatible with the GDPR and the GDPR Decree, and (ii) opened a 60-day public consultation procedure in connection with those compatible provisions.

Article 21(1) GDPR Decree established that the Italian DPA would only review the GDPR compliance of those general authorisations that relate to processing situations covered by articles 6(1)(c), 9(2)(b) and (4), and Chapter IX of the GDPR, meaning processing:

- Necessary for compliance with a legal obligation to which the controller is subject;

⁴ Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972>.

⁵ Under the previous article 26 of the Data Protection Code, sensitive data (which are now "special categories of personal data") could only be processed with (i) the data subject's prior written consent; and (ii) the Italian DPA's prior authorisation. Only in the special cases listed in article 26(4) was processing permitted with just the Italian DPA's authorisation.

- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or of genetic data, biometric data or data concerning health; or
- That is made in relation to particular sectors, such as specific employment relationships, or of personal data from archives, registers, lists, instruments and documents kept by public registries, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Therefore, the Italian DPA only reviewed general authorisations 1/2016 3/2016 6/2016, 8/2016 and 9/2016, which concerned the processing of sensitive (now special categories of) personal data: within employment contexts; by associations, foundations, churches, or religious associations or communities; by private investigators; and concerning processing of genetic data or for the purposes of scientific research.

In identifying those provisions that were compatible with the GDPR, the Italian DPA made a number of other statements. For example:

- The Italian DPA has set out specific modalities for the processing of special categories of personal data during the **pre-hiring phase**, providing, *inter alia* as follows:
 - Pre-hiring questionnaires must request only limited information that is strictly necessary to create the employment relationship, also taking into account the specific responsibilities or professional roles at issue (also from an employment law perspective, Art. 8 of Law No. 300/1970 prohibits enquiries on facts that are not relevant for the purpose of assessing the worker's professional aptitude);
 - If a **candidate's CV includes data** that is irrelevant for such purpose, those reading the CV must abstain from using the irrelevant information;
 - **Genetic data cannot be processed** for the purposes of establishing whether the candidate is professionally suitable, not even with the candidate's consent;
- In relation to processing **during the employment relationship**, the Italian DPA has stated *inter alia* the following:
 - The employer can process data that reveals **political opinion or membership of a labour union** or the exercising of related responsibilities exclusively for purposes relating to use of permits/leave time and the exercise of union rights (e.g. salary withholdings);
 - Making express reference to the principle of necessity, the Italian DPA has provided that for the purposes of carrying activities in polling stations during elections, a certification from the polling station's president will suffice and therefore the employer cannot request any document which would reveal the employee's political opinion.

Achieving the same safeguard as above, the Italian DPA had already previously stated that the employer merely needs to inform the labour union that one of its employees has revoked his or her affiliation to the labour union, and thus — the Italian DPA deemed it unlawful for the employer to reveal the employee's concurrent enrolment in another labour union (see doc. web no. 9065999, **newsletter dated 7 December 2018**)⁶.

- In all authorisation reviewed, the Italian DPA eliminated those provisions that had merely stated that data could not be stored "*for a period exceeding that necessary.... to pursue the purposes mentioned therein*".

Article 20(5) of the GDPR Decree specifies that breaches of the provisions of general authorisations are subject to the same administrative fines as would be imposed for breaches of rules of professional

⁶ At link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9065999>.

practice under article 166 of the Data Protection Codes (as already mentioned, a fine of up to €20 million or 4% of global annual revenues).

The general authorisations that the Italian DPA had adopted prior to 19 September 2018, related to processing not within the above, ceased to be in effect from that date forward (article 21(3) of the GDPR Decree⁷).

THE KINDS OF PROCESSING THAT ARE SUBJECT TO IMPACT ASSESSMENT

In accordance with its duty under article 35(4) of the GDPR, the Italian DPA in a decision of 11 October 2018 set out a **list of the kinds of personal data processing operations** that would be **subject to a data protection impact assessment (a "DPIA")**⁸. As acknowledged by the Italian DPA, the DPIA implements the considerations of the European Data Protection Board and is without prejudice to the guidelines of WP 248, rev. 01⁹, with a view towards harmonisation and consistent application of the GDPR also in cross-border processing.

The non-exhaustive list of the data processing operations by the Italian DPA¹⁰ includes:

- Processing that implies the **profiling of** the data subjects, and activities involving predictions, in relation to, for example, professional performance, economic condition, health, reliability, relocations;
- **Automated** processing with the aim of making decisions that prevent exercise of a right or the use of an asset or service or that cause the expiry of the status as a party under a contract (among these the Italian DPA includes a bank's screening of its customers by using data stored in a centralised risk databank);
- Large-scale processing of **highly personal data**, such as data relating to a data subject's family status or private sphere (including electronic communications and related data the confidentiality of which must be protected), data concerning physical location, and financial data that could be used fraudulently;
- More generally, processing of special categories of personal data pursuant to Article 9 of the GDPR or data relating to criminal convictions and offences pursuant to Article 10 of GDPR **when interconnected with other** personal data collected for other purposes;
- Processing that implies the large-scale, electronic exchange of data **between different data controllers**.

Thus, the existing, widely-used practice providing for a broad application of the DPIA has been confirmed.

The above list also includes processing in the context of an employment relationship performed using technology systems (such as video surveillance and **geolocalisation**) that allow remote monitoring of the employees. Use of such systems must also be agreed with the labour union representatives and/or the Labour Inspectorate pursuant to Article 4 of Law 300/1970, as amended by Article 23 of Legislative Decree 151/2015, except in relation to instruments used by the employee to perform the working activity and for instruments that record access and physical presence at the workplace.

⁷ Authorisations Nos. 2, 4, 5 and 7/2016. These covered: (i) the processing of court data by private entities, public economic entities and public entities; (ii) the processing of data that might reveal information on health or sexual life, (iii) the processing of sensitive data by the self-employed professionals; and (iv) the processing of sensitive data by various categories of data controller.

⁸ The list is available at:

<https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto>.

⁹ Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

¹⁰ The Italian DPA expressly provides that the list is not exhaustive, and may be amended or supplemented also on the basis of the outcome of the first phase of application of the GDPR.

We highlight a recent ruling in the judicial employment law dispute involving the **Foodora** bicycle couriers who worked using an **app installed on their smartphones**. The couriers had sought compensation for damages as a result of the alleged breach of Article 4 of Law 300/1970, as well as of Articles 7, 11 and 171 of the Data Protection Code previously in force, given they had not been clearly and fully informed of the nature of the data processed, of the characteristics of the device and of the monitoring and the circumstances when the geolocalisation could be deactivated during work performance. In the first instance proceedings all of the couriers' claims had been denied by the Court of Turin (Ruling No. 778/2018).

The Court of Appeal of Turin, with Ruling No. 26/2019 of 11 January 2019 (for which the opinion and reasoning has not yet been issued) granted the couriers' appeal in part, recognising they should receive the same compensation as employees on the basis of the parity of treatment principle pursuant to Article 2 of Legislative Decree 81/2015, although the Court did not classify their work relationship as subordinate employment. **In relation to the privacy claims, the Court of Appeal did not reverse the first instance ruling**, which held that the notice given to the couriers was not overly general and that *"the apps on the smartphone were used by the plaintiffs to perform the work activities and as such they did not require an agreement with the labour union representatives."*

The couriers, nevertheless, have publicised that they in December 2018 **filed a complaint with the Italian DPA pursuant to Art. 77 of the GDPR**, bringing forth new claims, including in relation to the continuous and unauthorised monitoring and geolocalisation of the couriers even outside of their working hours.

THE MEMORANDUM OF UNDERSTANDING MADE BETWEEN THE ROME PROSECUTION SERVICE AND THE REGULATOR

On 8 January 2019, the Rome prosecution service and the Italian DPA entered into a memorandum of understanding for the implementation of the new rules on personal data protection that the GDPR Decree had introduced (the "**MoU**").¹¹ The MoU is effective for a period of two years, and subject to automatic renewal.

It governs how effect will be given to articles 167(4), 167-*bis*(3), and 167-*ter*(2), of the Data Protection Code, as introduced by the GDPR Decree. Those provisions require public prosecutors to notify the Italian DPA "without delay" if it learns that specific offences may have been committed in connection with personal data protection, offences which are set out in the aforementioned articles. The intention is to ensure that investigations into possible offences proceed quickly, and to ensure that the criminal and administrative processes for punishing breaches of the law benefit from effective coordination. Accordingly, the MoU provides that:

- It is the public prosecutor in charge of a particular investigation that informs the Italian DPA, rather than the head of the prosecution service, so that information is shared quickly and without bureaucratic deferrals; and
- As soon as the suspect being investigated and their counsel have been formally notified that the preliminary investigations have been completed, the public prosecutor in charge must notify the Italian DPA of such evidence as would be necessary for it to examine whether there have been breaches of the law on personal data protection in connection with the offence.¹² This procedure is intended to enable the Italian DPA to act more efficiently, while ensuring that appropriate investigative secrecy is maintained.

¹¹ The MoU may be examined at:

<https://www.garanteprivacy.it/documents/10160/0/Protocollo+tra+Procura+di+Roma+e+Garante+privacy+-+8+gennaio+2019>.

¹² Article 1(2) of the MoU also specifies that "the notice referred to in paragraph 1 shall contain all the evidence necessary for the Regulator to commence any administrative proceedings in connection with the commission of the offence".

AUTHORS

Simonetta Candela
Partner, Milan
T +39 02 8063 4245
E simonetta.candela@cliffordchance.com

Luciano Di Via
Partner, Rome
T +39 064229 1265
E luciano.divia@cliffordchance.com

Carlo Felice Giampaolino
Partner, Rome
T +39 064229 1356
E carlofelice.giampaolino@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Piazzetta M.Bossi, 3, 20121, Milano, Italia

© Clifford Chance 2019

Clifford Chance Studio Legale Associato

Fabio Guastadisegni
Partner, Milan
T +39 02 8063 4353
E fabio.guastadisegni@cliffordchance.com

Marina Mobiglia
Senior Associate, Milan
T +39 02 8063 4339
E marina.mobiglia@cliffordchance.com

Andrea Tuninetti Ferrari
Senior Associate, Milan
T +39 02 8063 4435
E andrea.tuninettiferrari@cliffordchance.com

Alessandro Sciarra
Associate, Rome
T +39 064229 1384
E alessandro.sciarra@cliffordchance.com

Iolanda D'Anselmo
Trainee Lawyer, Milan
T +39 02 8063 4294
E iolanda.danselmo@cliffordchance.com

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Doha • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • Jakarta* • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

NETWORK

Maxime D'Angelo Petrucci
Avocat, Paris
T +33 1 4405 5167
E maxime.dangelopetrucci@cliffordchance.com

Megan Gordon
Partner, Washington DC
T +1 202 912 5021
E megan.gordon@cliffordchance.com

Jonathan Kewley
Partner, London
T +44 207006 3629
E jonathan.kewley@cliffordchance.com

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

Dessislava Savova
Partner, Paris
T +33 1 4405 5483
E dessislava.savova@cliffordchance.com

Grégory Sroussi
Avocat, Paris
T +33 1 4405 5248
E gregory.sroussi@cliffordchance.com

Richard Jones
Director of Data Privacy, London
T +44 20 7006 8238
E richard.jones@cliffordchance.com