ITALY IMPLEMENTS THE GDPR

On **19 September 2018**, Legislative Decree no. 101/2018 (the "**Decree**") enters into force. By way of the Decree, Italy is updating its Personal Data Protection Code (Legislative Decree no.196/2003, the "**Code**") following the entry into force of the General Data Protection Regulation ("**GDPR**")[1]. The new version of the Code refers to the GDPR as the key regulation for the processing of personal data, which must respect human dignity and fundamental rights and freedoms of natural persons. The Decree also makes significant reforms in relation to administrative and criminal fines and makes the resolution of pending sanctions proceedings easier.

Key issues

- Heavier sanctions to safeguard minors as regards consent, recipients of "unsolicited communications" and sensitive data
- 14 is the minimum age at which consent can be given
- Criminal sanctions and easier resolution of pending litigation
- Ethical standards for the processing of personal data within employment relationships
- Specific obligations for the operators of electronic communications services
- Cumulation of notification obligations under the GDPR and the NIS Directive

THE NEW PRIVACY CODE

SUMMARY OF THE REFORMS

- **Minors:** for **consent to the processing of personal data in relation to the offer of information society services directly to a child**, 14 is the minimum age in Italy. Italy has exercised the power set forth in the GDPR which sets 16 as the minimum European standard but allows member states to lower the threshold.
- **Genetic, biometric and health data:** implementing art. 9, paragraph 4 of the GDPR, the Decree provides for the adoption of safeguards for the processing of genetic, biometric and health data by the authority for the protection of personal data (the "**Data Protection Authority**") to be updated every two years, compliance with which is a **condition for the lawfulness of the processing**. The Data Protection Authority will also identify simplified methods for giving consent, when required. Moreover, the Decree introduces a general ban on the dissemination of biometric, genetic and health data (a ban is already present in the Code for the latter category of data). This means that personal data cannot be disseminated to indeterminate persons and must not be placed at anyone's disposal or made available for consultation.

  The Decree allows the use of biometric data in order to implement procedures for restricted access to personal data within the technical and organisational measures for the protection of data that controllers must implement under art. 32 of the GDPR.

[1] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- **Data relating to criminal convictions and offences** (when the processing is not carried out under the control of official authority): the processing of these data is allowed if authorised in accordance with a provision of the law or a regulation, if the law so provides, which should provide appropriate safeguards for the rights and freedoms of the persons concerned. Without this authorisation, the processing in question and the related safeguards are determined by a decree of the Ministry of Justice, following consultation with the Data Protection Authority.
- **Restrictions on the rights of the persons concerned** (articles 15-22 GDPR: access, rectification, the "right to be forgotten", restriction of processing, portability, objections and safeguards within the sphere of automated decision-making): the exercise of these rights against the data controller or by way of a complaint to the Data Protection Authority is restricted in those limited cases in which it could prejudice other rights or relevant interests (for example, interests safeguarded by anti-money laundering laws). The Decree provides that a "reasoned notification" must be delivered without delay to the person concerned in relation to the restriction, delay or exclusion of these rights.
- **Delegation of functions and tasks:** the data controller or processor, where appointed, can, on its own initiative, assign to the natural persons operating under its own authority tasks and functions relating to the processing.
- **"*Robinson List*":** the Decree confirms the ban on data processing for so-called "direct marketing" purposes in relation to personal data on public paper or electronic lists when the persons concerned have exercised their right to raise an objection by way of registering with the Public Register of Objections.
- **Guidelines:** exercising the powers provided for every member state by art. 58, paragraph 6 of the GDPR, the Decree grants to the Data Protection Authority the power to adopt guidelines on the organisational and technical measures to implement the principles of the GDPR, including the principle of minimisation of the processing of the data.
- **Ethical standards of behaviour in employment relationships:** the Data Protection Authority must also promote the adoption of ethical standards for data processing within employment relationships and also provide for specific methods for providing information to the person concerned, in the exercise of the powers provided for every member state by art. 88 of the GDPR. Compliance with the ethical standards, which will be published in the *Gazzetta Ufficiale della Repubblica Italiana* by way of decree of the Ministry of Justice, **will constitute a condition for the lawfulness** of the processing.
- **Processing of data contained in CVs without need for consent:** the Decree expressly states that a privacy statement must be provided to the senders of CVs sent as spontaneous applications upon first contact with them after delivery of the CVs. Within the limits of the purposes of the enforcement of pre-contractual measures adopted at the request of the person concerned (art. 6(1)(b) GDPR), consent to the processing of personal data in the CVs is not required.

Administrative Sanctions

The Decree provides a heavier fine of up to **Euro 20,000,000.00 or, for enterprises, up to 4% of the global annual turnover**, whichever is higher, for the breach, amongst other things, of:

- the provisions regarding the consent of minors;
- the provisions on so-called "unsolicited communications";
- the provisions on the processing of data relating to the traffic of subscribers and users processed by the supplier of a public network of communications or a communications service accessible to the public;
- the safeguards concerning the processing of genetic, biometric and health data;
- the ethical standards for specific types of processing, including those relating to the processing of personal data within an employment relationship;
- the IVASS (Institute for Insurance Supervision) measures relating to the procedures and the operating methods of the database of claims established to prevent and combat fraudulent behaviour in the sector of compulsory third party insurance; and
- the ban on communicating to third parties, transferring and circulating the personal data of persons registered with the Public Register of Objections for the purposes of advertising, sales or conducting market research or commercial communications not relating to the activities, products or services offered by the data controller.

Criminal Sanctions

As regards criminal sanctions, it is to be noted that even though the first draft of the Decree sought to bring about a massive decriminalisation by radically reducing the criminal sanctions, the new Decree still contains offences: some of them were already in the "old" Code whilst others are new.

The Decree, in any case, confirms the willingness **not to include** offences relating to the protection of personal data in the list of relevant offences under Law 231/2001, i.e. those in relation to which corporate entities are vicariously liable for the criminal conduct of their employees.

- **Unlawful processing of personal data**

  The provision set out at art. 167 of the Code has been preserved but is currently applicable not only to behaviour driven by the desire to gain profit, as previously, but, rather, is worded so as to include also behaviour engaged in with the intention of causing damage to others.

  The offence is punishable with a prison term of between six and 18 months. The sanction is increased to a prison term of up to three years where *special categories of data* (pursuant to art. 9 of the GDPR) and *data relating to criminal convictions and offences* (pursuant to art. 10 of the Regulation) are used in order to gain a profit for oneself or others or in order to cause damage to the person concerned and also when the same data are processed and there are high risks for the performance of a task of public interest that causes damage to the person concerned.

  The Decree provides for a flow of information between the Public Prosecutor and the Data Protection Authority such that the Public Prosecutor informs the Data Protection Authority without delay when

he/she has information on a crime as per art. 167 of the Code and the Data Protection Authority sends to the Public Prosecutor, by way of a reasoned report, the documentation collected during the investigation where a crime is presumed to have been committed.

In order to prevent the sanction from being excessively heavy, where the administrative sanction is also applicable to the case at hand the penalty must be reduced.

- **Unlawful notification and circulation of personal data subject to large-scale processing**

  Art. 167-*bis* of the Code introduces a new offence aimed at punishing large-scale circulation of data in the event of non-compliance with specific legal requirements (for example, where the person concerned has not given its consent) when driven by the desire to cause damage to others or gain a profit for oneself or others.

  The breaches are punished with a prison term of between one and six years but, in the event of the joint application of an administrative sanction, the sanction must be reduced.

- **Fraudulent acquisition of personal data subject to large-scale processing**

  A further criminal sanction can be found at art. 167-*ter* of the Code, which punishes behaviour by anyone who, for the purpose of gaining a profit or causing damage to others, fraudulently acquires an automated archive or a substantial part of one containing personal data subject to large-scale processing. The provision is closely connected to art. 167-*bis* and, in this case, the prison term is one to four years.

- **False statements to the Data Protection Authority and interrupting the performance of tasks or the exercise of the powers of the Data Protection Authority**

  Art. 168 of the Code, which punishes false declarations or statements to the Data Protection Authority with a prison term of six months to three years, has been retained.

  Further, anyone who intentionally causes an interruption to, or disturbs the regular conduct of, proceedings before the Data Protection Authority or its investigations can be punished with a prison term of up to one year.

- **Non-compliance with the measures of the Data Protection Authority**

  The offence set out at art. 170 of the Code has been retained even though a proposal was initially made to repeal it. The decree provides for a prison term of three months to two years.

- **Breaches of the provisions regarding remote monitoring and investigations into workers' opinions**

  Art. 171 of the Code concerning breaches of employment law has been retained. The behaviours subject to sanctions are the use of instruments intended to monitor the activities of workers, the installation of so-called potential surveillance devices without the prior agreement of internal works councils/employees' representatives or the authorisation of the Labour Inspectorate (art. 4 Law no. 300/1970, the so-called Workers' Statute), and investigations into facts not relevant to the assessment of the professional aptitude of workers (art. 8 Law no. 300/1970). Unless such actions constitute a more serious offence, these behaviours are

punishable with a fine of Euro 154.00 to 1,549.00 or imprisonment of 15 days to one year. In more serious circumstances, the fine plus imprisonment plus publication of the order finding criminal liability may apply. The Court may increase the fine by up to five times if the base fine is ineffective because of the economic circumstances of the employer.

- ***Favor rei***

  As regards the *favor rei*, art. 24 of the Decree points out that the administrative sanctions replacing the criminal ones apply to the breaches committed prior to 19 September 2018 relating to the crimes that have been decriminalized, provided that no judgment has already become final and binding. In the latter case, there could be a revocation by the enforcement judge because the law no longer qualifies the act as an offence.

EASIER RESOLUTION OF LITIGATION

The Decree provides for the possibility to resolve sanctions proceedings pending as at 25 May 2018, which have not been adjudicated by an order-injunction, by a payment at a reduced rate of a sum amounting to two-fifths of the minimum penalty.

To this end, **the payment must be made within 90 days of 19 September 2018.** Once this time limit has elapsed, and if no defence submissions have been presented, the Decree provides that the papers by means of which the breach was communicated, or the immediate complaint was made, qualify as an order-injunction.

OBLIGATIONS FOR OPERATORS OF ELECTRONIC COMMUNICATIONS SERVICES ACCESSIBLE TO THE PUBLIC

The Decree confirms the obligation of operators in the electronic communications sector (for example, suppliers of telephone services or internet services) to adopt appropriate measures for the protection, amongst other things, of personal data relating to traffic and location and to ensure the implementation of a data security policy.

In line with the principles of clarity in communications with interested parties set forth in the GDPR, the Decree specifies that the **information policy provided to subscribers** and, where possible, to users relating to any **risks of breach of security of the network**, already obligatory in the "old" Code, must **use language that is clear, appropriate and adequate for the category and the age group of the person concerned, with particular attention necessary in the case of minors**.

The **obligation to notify security incidents** to the *Computer Security Incident Response Team* (CSIRT), imposed by the so-called **NIS Directive**[2], of operators of essential services does not, however, apply to operators of electronic communications services[3], subject to specific sectorial obligations. The essential services taken into consideration by the NIS Directive and the

[2] Directive (EU) 2016/1148 of the European Parliament and Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. This Directive was recently implemented in Italy by way of Legislative Decree no. 65/2018, as reported in our updated document available via this link.

[3] To this category of exempted subjects are added suppliers of public communications networks as well as suppliers of trust services (for example, suppliers of electronic signature services) as per the eIDAS regulation (Regulation (EU) 910/2014 of the European Parliament and Council of 23 July 2014 concerning electrical identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

implementing Legislative Decree no. 65/2018 are, amongst others, banking, financial markets, energy, digital services and infrastructures, transport and healthcare.

As regards other **operators**, the Working Party under article 29 for the protection of data[4] warned of the **possibility that a security incident could also determine a breach of personal data**, and make it necessary to send a separate notification to the Data Protection Authority under art. 32 GDPR (a so-called data breach) in addition to the notification under the NIS Directive.

In order to gain an overview of the obligations to give notice of security incidents and breaches of data, including within the field of payment services, please consult our recent updated document via this link.

[4] As regards the notification obligation in respect of personal data breaches, please consult our updated document via this link.

AUTHORS

Carlo Felice Giampaolino
Partner, Rome

T +39 064229 1356
E carlofelice.giampaolino@cliffordchance.com

Simonetta Candela
Partner, Milan

T +39 02 8063 4245
E simonetta.candela@cliffordchance.com

Jean-Paule Castagno
Counsel, Milan

T +39 02 8063 4317
E jean-paule.castagno@cliffordchance.com

Pasquale Grella
Senior Associate, Milan

T +39 02 8063 4289
E pasquale.grella@cliffordchance.com

Marina Mobiglia
Senior Associate, Milan

T +39 02 8063 4339
E marina.mobiglia@cliffordchance.com

Alessandro Sciarra
Lawyer, Rome

T +39 064229 1384
E alessandro.sciarra@cliffordchance.com

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

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

www.cliffordchance.com

Clifford Chance, Piazzetta M.Bossi, 3, 20121 Milan, Italy

Clifford Chance Studio Legale Associato

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

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.