MACCHI di CELLERE GANGEMI

27 October 2017

THE NEW EU GENERAL DATA PROTECTION REGULATION & UK - ITALIAN FILING OBLIGATIONS

KEY CHANGES AND NOTIFICATION REQUIREMENTS IN UK AND ITALY

With data increasingly flowing without boundaries across Member States, the General Data Protection Regulation (GDPR) has attracted a huge amount of attention and is the culmination of years of efforts by EU institutions to harmonise data protection across the European territory.

The GDPR will replace the Data Protection Directive (95/46/EC) on the 25th of May 2018 and is set to bring significant changes to the framework currently in place.

In view of May 2018, businesses and organisations are urged to begin preparations and review existing practices to comply with the new regulation. This note summarises some of the key points of the GDPR and the current UK obligations under the Data Protection Act and in Italy.

Expanded Territorial Scope

The GDPR will be directly applicable in all EU Member States without the need for transposition. In addition, it is likely that the GDPR will apply in the three members of the European Economic Area (EEA) that are not members of the EU (Iceland, Lichtenstein and Norway) through incorporation into Article 7 of and Annex XI to the EEA Agreement.

Its territorial scope will however extend beyond EU data controllers and processors, to encompass any company outside the EU which is targeting consumers in the EU (and thus continue to be relevant even in the case of a so-called "*Brexit*" by the UK).

Non-EU data controllers and data processors will be required to comply with the GDPR if they either:

- '*Offer goods or services*' to data subjects in the EU.
- '*Monitor behaviour*' of data subjects within the EU.

Registrations and Data Protection Officers (DPO)

Instead of registering with a 'supervising data protection authority', the GDPR will require businesses to maintain detailed documentation, recording their processing activities. In certain circumstances, data controllers and processors must designate a DPO to facilitate and ensure accountability.

In the UK, the Data Protection Act 1998 currently requires every 'data controller' (e.g. company, firm, organisation, sole trader) who is processing personal information to register with the ICO (unless special exemption applies), and it is expected that this requirement will continue to

apply following the enactment of the GDPR (see below).

Accountability and Privacy by Design

A welcome change for data controllers is the removal of the general requirement to notify the supervising authority of a controller's data processing activities and to seek approval from the supervising authority in some circumstances. On the other hand, the GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to, in addition to - inter alia - maintaining detailed documentation, (i) conduct mandatory data protection impact assessments and mandatory prior consultations in certain circumstances of high risks to data subjects; and (ii) implement data protection by design (e.g. when creating new products, services or other data processing activities) and by default (e.g. data minimisation). The GDPR adopts a risk-based approach to compliance, under which businesses bear responsibility for assessing the degree of risk that their processing activities pose to data subjects.

Role of Data Processors

Under the GDPR, data processors will for the first time have direct compliance obligations including strict data breach notification obligations, a shift likely to increase the cost of data processing services and impact how data protection matters are dealt with in commercial agreements.

Consent

The Data Protection Directive distinguished between ordinary and explicit consent. The GDPR requires a much higher standard of consent than in the past, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed. Consent can be withdrawn at any time (it must be as easy to withdraw consent as to give it) and the burden of proof for validly obtained consent lies on the data processors and controllers. Businesses that have been able to rely on implied consent, in particular, and all businesses that have relied on consent as a legal basis for data processing in general, will have to carefully review their future practices.

Due attention and careful consideration should also be given to mechanisms of parental consent, an area likely to create inconsistencies throughout the territory (Member States may, at their discretion, be able to lower the age of consent from 16 to 13).

Fines and Enforcement

The GDPR establishes a severe two-tiered approach to penalties for breach which enables supervising authorities to increase their enforcement powers imposing fines of up to the higher of: (i) 4% of the annual worldwide turnover of the preceding financial year; and (ii) 20 million euros (for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers).

Violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default, can attract a fine of up to the higher of 2% of the annual worldwide turnover of the preceding financial year and 10 million euros.

Fair Processing Notes

Data controllers must provide transparent information in a clear and accessible format to data subjects, at the time the personal data is obtained. Existing forms of fair processing notice will have to be re-examined as the requirements in the GDPR are more detailed than those in the current Directive.

Data Breach Notifications

Businesses must notify all data breaches to the supervising authority without undue delay and, where feasible within 72 hours of awareness, unless the data breach is unlikely to result in a risk to the individuals. In cases of high risk, the data controller must also notify the affected data subjects without undue delay. Businesses will need to develop and implement data breach response procedures. The Article 29 Working Party is due to publish guidance on notifications of data breaches.

One-Stop-Shop

The 'One-Stop-Shop' mechanism is one of the key elements of the GDPR. It allows businesses present in more than one Member State to deal with a single lead supervising authority. It is then for the lead supervising authority to work with all other concerned authorities. In cases of failed cooperation, if the concerned authorities cannot agree on a decision, the matter is referred to the European Data Protection Board (EDPB). Complications are however predicted to arise in the determination of the single lead authority, in anticipation of which the Article 29 Working Party has adopted its final guidelines.

European Data Protection Board

An independent EDPB is to replace the Article 29 Working Party and will comprise the EDP Supervisor and the senior representatives of the national data protection authorities. Its role includes issuing opinions and guidance, ensuring consistent application of the GDPR and reporting to the Commission.

Binding Corporate Rules (BCRs)

The GDPR formally recognises BCRs for controllers and processors as a means to lawfully transfer personal data out of the European Economic Area (EEA). They will still require the supervising authority's approval, but the approval process should become less onerous than the current system.

Data Subject's Rights

The GDPR strengthened the rights of data subjects. These include:

- (i) the *right to erasure* or the right to be 'forgotten', whereby individuals will have the right to request that businesses delete their personal data in certain circumstances (e.g. after withdrawal of consent or where the data is no longer necessary);
- (ii) the *right to object to profiling*, whereby individuals will have the right to object to their personal data being processed. Profiling includes most forms of online tracking and behavioural advertising, making it harder for

businesses to use data for these activities. The fact of profiling must be disclosed to the data subject, and a mandatory data protection impact assessment is required;

- (iii) the *right to data portability*, whereby data subjects have a right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format and have the right to transmit those data to another controller. In general cases of data subject access data request, businesses will have to reply within one month from the date of receipt of the request and provide more information than required under the Data Protection Directive.

UK Registration (Obligation to Notify) under the Data Protection Act

The Data Protection Act 1998 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. Section 18 of the Act lists what information must be provided in notifying the ICO.

UK Register of Data Controllers

More than 400,000 organisations are currently registered at the ICO. The cost of registration is generally £35, but can reach £500 in the cases of a public authority with more than 249 members of staff, or if you have a turnover of £25.9 million and more than 249 members of staff.

UK Data Protection Enforcement Action

The Commissioner is responsible for enforcing the data protection regime. Enforcement action is generally undertaken following a complaint from a data subject. Where it finds a breach, the Commissioner may serve data controllers with (i) information notices, requiring data controllers to provide information about their processing operations (unless the information is self-incriminating or the subject of legal privilege); (ii) special information notices; or (iii) enforcement notices, requiring data controllers to comply with the data protection principles. The Commissioner has inspection powers (which need the support of a warrant from the court to be exercised), and a power to impose fines up to a maximum of £500,000 (a threshold that is going to be significantly raised under the GDPR) in cases of serious contraventions of the Data Protection Act (section 55A). As an alternative to enforcement through the Commissioner, an individual may apply to an English court to enforce his rights under the Act.

Registration with the Italian Data Protection Authority

Notification of processing to Italian Data Protection Authority (Garante per la Protezione dei Dati Personali, "IDPA"), is presently mandatory only whenever the processing concerns any of the following:

a) genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network;

b) data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods,

epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, HIV-positivity, organ and tissue transplantation and monitoring of health care expenditure;

c) data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character;

d) data processed by means of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users;

e) sensitive data stored in data bases for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys;

f) data stored in ad-hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

Notification shall be submitted to the IDPA in advance and once only, regardless of the number of operations to be performed and the duration of the processing (notification may refer to one or more processing operations for related purposes).

The notification describes the main features of the processing (e.g. categories of data processed, purposes of the processing, place where the processing is carried out, transfer of data outside the EU, security measures implemented) and is subject to the payment of a governmental fee of €150.

Stefano Macchi di Cellere
Partner
Macchi di Cellere Gangemi LLP – London
s.macchi@macchi-gangemi.com

Salvatore Orlando
Of-Counsel
Rome office
s.orlando@macchi-gangemi.com

Laura Liberati
Senior Associate
Rome office
l.liberati@macchi-gangemi.com

Macchi di Cellere Gangemi

LONDON
33 St. James's Square
SW1Y 4JS London
Tel: +44 (0) 20 3709
Fax: +44 (0) 20 3709 6014
london@macchi-gangemi.com

ROME
via G. Cuboni, 12
00197 Rome
Tel: +39 06 362141 6000
Fax: +39 06 3222159
roma@macchi-gangemi.com

MILAN
via G. Serbelloni, 4
20122 Milan
Tel: +39 02 763281
Fax: +39 02 76001618
milano@macchi-gangemi.com

VERONA
via Nizza, 20
37121 Verona
Tel: +39 045 8010911
Fax: +39 045 8036516
verona@macchi-gangemi.com

BOLOGNA
via Calcavinazzi, 1/d
40121 Bologna
Tel: +39 051 0953112
Fax: +39 051 0953119
bologna@macchi-gangemi.com

MODENA
Strada delle Fornaci, 20
41126 Modena
Tel: +39 059 2923203
Fax: +39 059 346651
modena@macchi-gangemi.com

PARIS
Avenue Hoche, 38
75008 Paris
Tel: +33 (0) 1 53757900
Fax: +33 (0) 1 53750015
paris@macchi-gangemi.com