The EU General Data Protection Regulation: a look at the provisions that deal specifically with cross-border situations

This post has been written by Martina Mantovani.

On 4 May 2016, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, or GDPR) was published on the Official Journal. It shall apply as of 25 May 2018.

Adopted on the basis of Article 16(2) TFEU, the Regulation is the core element of the Commission's Data protection reform package, which also includes a Directive for the protection of personal data with regard to the processing by criminal law enforcement authorities.

The new measure aims at modernising the legislative framework for data protection, so as to allow both businesses and citizens to seize the opportunities of the Digital Single Market.

First and foremost, businesses will benefit from a simplified legal landscape, as the detailed and uniform provisions laid down by the GDPR, which are directly applicable throughout the EU, will overcome most of the difficulties experienced with the divergent national implementations of Directive 95/46/EC, and with the rather complex conflict-of-law provision which appeared in Article 4 of the Directive.

Nevertheless, some coordination will still be required between the laws of the various Member States, since the new regime does not entirely rule out the relevance of national provisions. As stated in Recitals 8 and 10, the GDPR 'provides a margin of manoeuvre for Member States' to restrict or specify its rules. For example, Member States are allowed to specify or introduce further conditions for the processing depending, *inter alia*, on the nature of the data concerned (Recital 53 refers, in particular, to genetic, biometric, or health-related

data).

Secondly, the new Regulation marks a significant extension of the extraterritorial application of EU data protection law, with the express intent of leveling the playing field between European businesses and non-EU established companies operatig in the Single Market. In delimiting the territorial scope of application of the new rules, Article 3 of the GDPR borrows on the case-law of the Court of Justice regarding Article 4 of Directive 96/45/EC. Pursuant to Article 3(1), the Regulation applies to any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, 'regardless of whether the processing itself takes place within the Union or not' (along the lines of the *Google Spain* case).

Moreover, Article 3(2) refers to the targeting, by non-EU established controllers and processors, of individuals 'who are in the Union', for the purposes of offering goods or services to such subjects or monitoring their behaviours. This connecting factor, further specified by Recital 23 in keeping with the findings of the Court of Justice in *Weltimmo,* is somehow more specific than the former 'equipment/means' criteria set out by the Directive (cfr. Opinion 8/2010 of the Working Party on the Protection of Individuals with regard to the processing of personal data, on applicable law).

One of the key innovations brought along by the GDPR is the so-called one-stop-shop mechanism. The idea, in essence, is that where a data controller or processor processes information relating to individuals in more than one Member State, a supervisory authority in one EU Member State should be in charge of controlling the controller's or processor's activities, with the assistance and oversight of the corresponding authorities of the other Member States concerned (Article 52). It remains to be seen whether the watered down version which in the end found its way into the final text of the Regulation will effectively deliver the cutting of red tape promised to businesses.

The other goal of the GDPR is to provide individuals with a stronger control on their personal data, so as to restore consumers' trust in the digital economy. To this end, the new legislative framework updates some of the basic principles set out by Directive 95/46/EC — which are believed to 'remain sound' (Recital 9) — and devises some new ones, in order to further buttress the position of data subjects with respect to their own data.

The power of individuals to access and control their personal data is strengthened, *inter alia,* by the introduction of a 'right to be forgotten' (Article 17) and a right to data portability, aimed at facilitating the transmission of personal data between service providers (Article 20). The data subject additionally acquires a right to be notified, 'without undue delay' of any personal data breach which may result in 'a high risk to [his or her] rights and freedoms' (Article 33).

The effective protection of natural persons in relation to the processing of personal data also depends on the availability of adequate remedies in case of infringement. The Regulation acknowledges that the infringement of the rules on the processing of personal data may result in physical, material or non-material damage, 'of varying likelihood or severity' (Recital 75). The two-track system has been maintained, whereby the data subject is entitled to lodge a complaint against the data controller or processor either with the competente courts (Article 79) or with the competent supervisory authority (Article 77). Furthermore, pursuant to Article 78, any legally binding decision of a supervisory authority concerning the position of a data subject — or the lack of thereof — may be appealed before the courts of the Member State where the supervisory authority is established.

The GDPR additionally sets forth an embryonic procedural regime for proceedings in connection with the alleged infringement of data protection legislation.

In the first place, it introduces two unprecedented special rules of jurisdiction, the application of which should not be prejudiced, as stated in Recital 147, by 'general jurisdiction rules such as those of Regulation (EU) No 1215/2012', ie, the Brussels I*a* Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (by the way, the primacy of the GDPR over Brussels I*a* could equally be asserted under Article 67 of the latter Regulation). Article 79 of the GDPR provides that the data subject who considers that his or her rights under the Regulation have been infringed, may choose to bring proceedings before the courts of the Member State where the controller or processor has an establishment or, alternatively, before the courts of the Member State where the data subject himself or herself resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers. Article 82(6) clarifies that the courts of the same Member State have jurisdiction over actions for compensation of the damage suffered as a result of the said

infringements.

Article 81 of the GDPR deals with *lis pendens*. If proceedings concerning the same activities are already pending before a court in another Member State, any court other than the one first seised has the discretion (not the obligation) to stay its proceedings. The same court may also decide to decline jurisdiction in favour of the court first seized, provided that the latter court has jurisdiction over the proceedings in question and its law permits the consolidation of related proceedings.

Finally, the Regulation includes a provision concerning the recognition and enforcement of 'any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data'. Pursuant to Article 48, such judgments or decisions may be recognised or enforced solely on the basis of an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State..

This provision mirrors the stance recently taken by some Member States and their representatives in connection to an important cross-border dispute, where a similar question had arisen, which was in fact the object of different solutions on the two sides of the Atlantic.

In fact, in the light of the approach taken by US law enforcement authorities, search warrants seeking access to personal data stored in European data centres are regarded as a form of compelled disclosure, akin to a subpoena, requiring the recipient of the order to turn over information within its control, irrespective of the place in which data is effectively stored. What matters is the sheer existence of personal jurisdiction over the data controller, that is the ISP who receives the warrant, which would enable criminal prosecutors to unilaterally order seizure of the data stored abroad, without necessarily seeking cooperation thorough official channels such as Mutual Legal Assistance Treaties.

Article 48 of the Regulation (EU) 2016/679 may accordingly be read as the EU counter-reaction to these law enforcement claims.