Published on *The National Law Review* https://natlawreview.com

A Data Processing Agreement is Not Always Enough

Article By:

Bartolome Martin

When expanding/ directing operations into Europe, foreign organizations often have questions about how to deal with the EU's ever-expanding regulatory framework. From a data protection perspective, it is often assumed that B2B operations do not trigger the extraterritorial applicability of EU data protection laws (mainly, Regulation (EU) 2016/679 or GDPR) and that it is sufficient to enter into data processing agreements with European data controllers. But is it really that simple?

Some context…

As raised above, one of the most salient elements of the GDPR is that it applies not only to processing operations carried out by controllers and processors established in the European Union, but also to certain processing operations carried out by controllers and processors established outside the Union. This is the case of the processing related to the active offering of goods or services to data subjects in the Union and the monitoring of their behavior, as far as it takes place within the Union (Article 3.2 of the GDPR).

However, what constitutes an active offering of goods or services, what constitutes monitoring the behavior of data subjects, and which authority is competent to supervise compliance with the regulation by these controllers are tricky questions to handle.

Some of these have been resolved by the European Data Protection Board (EDPB), the highest interpreter of the GDPR, which has clarified in its Guidelines 3/2018 on the territorial scope of the GDPR (Guidelines 3/2018), published prior to the aforementioned correction, and in its Opinion 04/2024 on the concept of a controller's main establishment in the Union under Article 4(16)(a) of the GDPR that:

- the GDPR only applies to processing operations carried out deliberately in the context of an active offer of goods or services to data subjects located in the EU (in application of the doctrine Pammer/Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof/Heller – Joined Cases C-585/08 and C-144/09, which is followed when analyzing whether or not the activity of an information society service provider is subject to the European rules on electronic commerce);
- the monitoring of the behavior of data subjects involves the tracking of their activity on the Internet or through other types of networks or technologies involving the processing of personal data, for example, through wearables or other smart devices, even if it is preparatory

processing necessary for third parties to carry out such monitoring (this is the view of several of the European data protection authorities, including the CNIL or the ICO, although there are judicial decisions at the national level that do not agree with this position); and that

- a controller or processor who is not established in the EU cannot benefit from the one-stop-shop mechanism that applies to a controller or processor who, being established within the territory of the EU, carries out cross border processing of personal data, so that any data protection authority knowing of a complaint or considering that a particular processing operation is being carried out in its jurisdiction may take action against such a controller or processor not established in the Union if it considers so appropriate and/or necessary (a controversial position that aims to avoid the forum shopping that would result from following other criteria, such as that of the location of the controller's or processor's representative in the Union, but which places those who operate from outside the EU in several Member States at a competitive disadvantage compared to those who do so transnationally from an establishment within the Union; something curious if we consider that the purpose of providing the GDPR with an extraterritorial nature was precisely to avoid situations of unfair competition by those who operate without being established in the Union).

The EDPB does not enter into the question regarding the applicability of supplementary national regulations to the activity of these controllers or processors established outside the EU, since, in relation to this, the national regulations themselves shall be followed, this being a matter, therefore, of private international law. However, many times, these supplementary laws are silent in this respect; something that may have undesirable consequences, given that national laws in some Member States regulate key issues in data protection matters, such as the statute of limitations for the infringements provided for in the GDPR or the sanctioning procedure to be followed by the authorities when exerting their authority.

The hitch…

With regard to data processors, the EDPB Guidelines 3/2018 determine that, when a processor established outside the EU takes part in activities carried out by controllers established within the EU, or outside the EU when the processing takes place in the context of the activities described in Article 3.2 of the GDPR, the processing of personal data carried out by them will be subject to the GDPR.

However, processors targeting EU markets are often unaware of their responsibilities when providing services to customers that process personal data for activities that fall within the scope of Article 3.2 GDPR. Sometimes, they may not even fully understand the nature of the personal data they are accessing in their capacity as data processors (for example, cloud hosting service providers).

As a result, while they may enter into data processing agreements with customers (and believe that this is sufficient to comply with their GDPR obligations), they may overlook that the same processing, when related to activities that fall within the scope of Article 3.2 GDPR, requires, in addition to having in place such an agreement, compliance with other GDPR processor-related obligations, such as: appointing a representative in the Union or keeping records of processing activities, and (this is something they particularly overlook) being subject to scrutiny by European data protection authorities.

In light of the above, in practice, processors must clarify with their customers whether their services are related to activities that fall within the scope of Article 3.2 GDPR, not only to be able to reflect this in the relevant data processing contract, but also to understand the implications of providing their services and to take additional compliance measures, as appropriate.

National Law Review, Volume XIV, Number 193