ONTIER

05th September 2017
#15

Index

SUPERVISORY AUTHORITIES AND THE ONE STOP SHOP

The GDPR introduces a number of significant changes in which national supervisory authorities in each member state will have greater enforcement powers including the power to levy bigger and more substantial fines on Data Controllers and Data Processors for failing to comply with the GDPR. To avoid Data Controllers and Data Processors having to deal with multiple supervisory authorities who may hand down varying decisions over the same issues, the Regulation will provide them with more certainty by introducing the “one stop shop” principle.

Current situation

Under Directive 95/46/EC, there is currently a competent national supervisory authority in each member state and Data Controllers (and not Data Processors) are subject to enforcement by the national supervisory authority within each member state where it carries out its processing activities. Each supervisory authority however, is only responsible for monitoring and enforcing compliance with local laws regarding the processing of personal data (the Directive is not directly applicable and had to be transposed into national law), with its own local investigative and effective powers and prescribed cooperation with other supervisory authorities from other member states. It was therefore common for Data Controllers to be subject to inconsistent decisions on the same issue from supervisory authorities across multiple member states. Data Processors are not subject to the Directive.

What's new?

Under the GDPR, each member state will still have its own competent supervisory authority to enforce the Regulation against both Data Controllers and Data Processors. What will be different is where a Data Controller or Data Processor processes personal data in more than one member state, instead of dealing with the supervisory authority in each member state in which they operate in (as per Directive 95/46/EC), they will now only have to deal with the supervisory authority in the member state of where its main establishment is based. That supervisory authority will be the lead supervisory authority (Lead SA) who will be responsible for monitoring the Data Controller/Data Processor's processing activities, handing down any decisions against them and dealing with the enforcement of any decisions relating to that Data Controller/Data Processor throughout the EU. This new concept is the "one stop shop" principle.

The essence of this principle is that the supervision of cross-border processing should be led by only one supervisory authority in the EU and so:

• ensures the GDPR is applied consistently;
• provides legal certainty; and
• reduces the administrative burden on Data Controllers and Data Processors who carry out cross-border data processing activities.

Main establishment is defined in Article 4(16) of the GDPR as:

a) for a Data Controller, "the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment"; and

b) for a Data Processor, "the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an

establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation".

In short, it is where the main processing activities and decision making of the Data Controller/Data Processor takes place.

Data controllers and Data Processors will predominantly be regulated for all GDPR compliance issues by a single supervisory authority across all its EU operations. If a business is located in only one member state but has processing activities that impact data subjects in other member states, it too will only have to predominantly deal with a single supervisory authority.

In its guidelines published in December 2016, the Article 29 Working Party ("WP29") makes it clear that Data Controllers and Data Processors are required to identify where its main establishment is themselves and which supervisory authority is its Lead SA. This can be challenged however, by a concerned supervisory authority if it feels that it is necessary to do so. The GDPR also does not allow "forum shopping" so businesses cannot claim to have its main establishment in one Member State if it has no effective or real exercise of management activity or decision making over the processing of personal data in that particular Member State.

It is envisaged under Chapter VIII of the GDPR that when a complaint is lodged by a data subject with a supervisory authority about a Data Controller or Data Processor, the supervisory authority must inform the Lead SA (if it is not the Lead SA) of that complaint "without delay". The Lead SA will then have three weeks to decide whether it will handle the complaint, taking into account of whether or not the Data Controller or Data Processor has an establishment in the Lead SA's member's state. If the Lead SA agrees to deal with the complaint, it will take the lead in the investigation into the matter.

Article 60 of the GDPR provides that the Lead SA must co-operate with the other supervisory authorities concerned in an endeavour to reach consensus and exchange all relevant information with each other. The Lead SA may also request the relevant supervisory authorities to provide mutual assistance under Article 61 and may conduct joint operations under Article 62. These forms of co-operations is particularly useful in situations where the Lead SA needs the assistance of another supervisory authority in monitoring or implementing a measure on a Data Controller or Data Processor in a different member state than the Lead SA and ensure there is consistency in its implementation throughout the EU.

Supervisory authorities must however, provide one another with mutual assistance in the performance of their duties and may carry out joint operations before a decision (which has been jointly agreed to by the Lead SA and all other applicable supervisory authorities concerned if it relates to cross-border processing activities) is handed down by the Lead SA.

It should be noted that the one stop shop principle only applies to a single Data Controller/Data Processors with cross border processing activities. Unless all decision are centralised in one country, a multinational organisation is unlikely to benefit from the mechanism. Recital 127 of the GDPR stipulates that each supervisory authority that is not the Lead SA should be competent to handle local cases where a Data Controller/Data Processor is established in more than one member state. Article 55 further confirms this by stating "Each supervisory authority shall be competent for the performance of the tasks

assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own member state".

In the 2016 guidelines, the WP29 states that the supervision of HR data connected to local employment requirements could fall to the supervisory authorities in the relevant member states. Another example where national supervisory authorities would have jurisdiction is if a multinational company has different operations established in different member states and each division has the power to make its own decision on data processing activities. In those circumstances, each operation will be subject to the supervisory authority where it is based.

What to do to adapt?

For businesses that only operate in a single member state and only process the personal data of data subjects residing in that member state, it will continue to interact with their local supervisory authority under the GDPR like it is currently doing under Directive 95/46/EC. Organisations that operate and/or have processing activities in more than one member state will have to adapt to interacting predominantly with the supervisory authority where their main establishment is as their Lead SA for the purposes of the GDPR. To do this, organisations will need to review their operations and determine which supervisory authority will be their Lead SA but should also bear in mind which other supervisory authorities may continue to have jurisdiction over them for matter specifically within its jurisdiction such as local employment matters. Where the organisation is a multinational company with multiple group undertakings, it will need to review where personal data is being processed and who is making decisions about the processing activities and determine whether they will still be in fact be subject to multiple supervisory authorities.

A practical example:

A Spanish citizen lodges a complaint with the Spanish supervisory authority relating to the cross-border data processing activities of a German company. In this instance, the 'one stop shop' principle will apply. As the German supervisory authority is the Lead SA with respect to the processing activities of the German company, the Spanish supervisory authority has to notify the German supervisory authority of the complaint. Upon such notification, the German supervisory authority will decide whether or not to take over the complaint from the Spanish supervisory authority. If it does, the German supervisory authority will be responsible for the decision and enforcement (if any) relating to the complaint raised about the German company. Any decisions made shall be agreed jointly between the German and Spanish supervisory authorities as well any other concerned supervisory authority, following a process of sharing draft decisions and exchanging relevant information. If the German supervisory authority decides not to take over the complaint, it shall be handled at local level by the Spanish supervisory authority instead.

A practical example:

A Spanish citizen lodges a complaint with the Spanish supervisory authority relating to the cross-border data processing activities of a German company. In this instance, the 'one stop shop' principle will apply. As the German supervisory authority is the Lead SA with respect to the processing activities of the German company, the Spanish supervisory authority has to notify the German supervisory authority of the complaint. Upon such notification, the German supervisory authority will decide whether or not to take over the complaint from the Spanish supervisory authority. If it does, the German supervisory authority will be responsible for the decision and enforcement (if any) relating to the complaint raised about the German company. Any decisions made shall be agreed jointly between the German and Spanish supervisory authorities as well any other concerned supervisory authority, following a process of sharing draft decisions and exchanging relevant information. If the German supervisory authority decides not to take over the complaint, it shall be handled at local level by the Spanish supervisory authority instead.

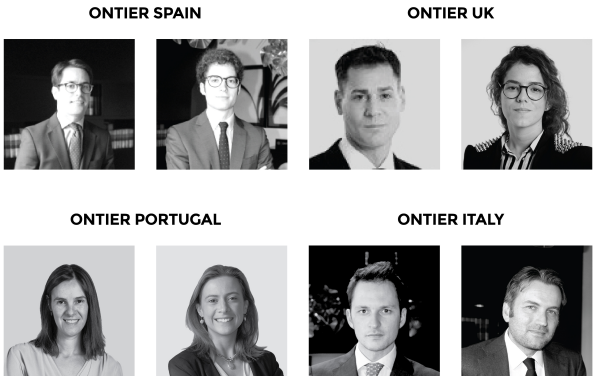
TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Derek Stinson (UK)
Paula Enríquez (UK)

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Luca Pardo (Italy)
Giulio Ciompi (Italy)



Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / **ITALY** / MEXICO / PERU / VENEZUELA
