WILLIAM FRY

// PRIVACY SOURCE

The Article 29 Working Party Guidelines on Identifying a Controller and Processor's Lead Supervisory Authority

In late December 2016, the Article 29 Working Party (now called the European Data Protection Board ("**EDPB**")) published the first tranche of eagerly awaited draft guidelines to assist organisations with the application and interpretation of certain chapters of the EU General Data Protection Regulation ("**GDPR**"). After a period of public consultation, the EDPB issued finalised guidelines on 5 April 2017.

The EDPB released three sets of finalised guidelines in relation to:

- the right to data portability;
- Data Protection Officers; and
- identifying a controller and processor's lead supervisory authority.

This InFocus article details the EDPB's guidelines concerning **identifying a controller's lead supervisory authority.**

Identifying a Lead Supervisory Authority

Controllers undertaking cross-border processing activities in the EU are required to identify the lead supervisory authority (the "SA") that will have primary responsibility for dealing with those activities. The process of identification may not always be straightforward and in some cases may be quite complex (e.g. for groups of companies see below). To assist with managing this process the EDPB has issued guidelines for identifying a controller or processor's lead SA.

In this article we explore the EDPB guidance for how an EU based controller can establish the identity of its lead SA, exploring scenarios where group processing activities of a controller might lead to it being subject to more than one lead SA, depending on where group decisions about the purposes and means of the processing are given final 'sign off'.

Background

The cooperation and consistency procedure or "one-stop shop" principle (the "OSS") is one of the cornerstones of the GDPR. The objective of the OSS is to reduce the administrative burden, uncertainty and inconsistency for controllers which existed prior to GDPR coming into effect.

Prior to GDPR, controllers "*established*" and processing personal data in more than one EU Member State were subject to the jurisdiction of the data protection SAs in each of these Member States. Often, these SAs were enforcing distinct data protection requirements, thereby producing diverse best practice guidelines and setting very different enforcement priorities.

The OSS eliminated these inconsistencies and allows the SA in the jurisdiction of the controller's "main establishment" to take the role of lead SA. In order to operate in this system, the controller needs to identify its lead SA.

When is a lead SA relevant?

Identifying a lead SA is relevant where a controller is carrying out cross-border processing of personal data. Article 4(23) of the GDPR defines 'cross- border processing' as either the:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the [European] Union where the controller or
- processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the [European] Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

For example, if a multinational has establishments in Ireland and the UK and the processing of personal data takes place in the context of activities of both establishments, then this will constitute cross-border processing. Cross-border processing can also occur where the same multinational only carries out its processing activity in the context of its establishment in Ireland. However, if the activity substantially affects, or is likely to substantially affect, data subjects in Ireland and the UK then this will also constitute cross-border processing.

Processing that "substantially affects"

According to the EDPB guidelines, controllers should assume a literal dictionary meaning of the words "substantially" and "affects", i.e. the processing should have some form of impact on data subjects in the respective Member States. So, cross-border processing takes place where:

- *that processing has some form of impact on individuals* in more than one Member State (processing with little or no effect on individuals does not qualify); and
- there is the likelihood of a substantial effect, not just an actual substantial effect. Note that "likely to" does not mean that there is a remote possibility of a substantial effect. The substantial effect must be more likely than not. On the other hand, it also means that individuals do not have to be actually affected: the likelihood of a substantial effect is sufficient to bring the processing within the definition of cross-border processing.

SAs will interpret "substantially affects" on a case by case basis. The factors that the EDPB will take into account, would include the context of the processing, the type of data, the purpose of the

- processing and factors such as whether the processing:
- causes, or is likely to cause, damage, loss or distress to individuals;
- has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity;
- affects, or is likely to affect individuals' health, well-being or peace of mind;
- affects, or is likely to affect individuals' financial or economic status or circumstances;
- leaves individuals open to discrimination or unfair treatment;
- involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children;
- causes, or is likely to cause individuals to change their behaviour in a significant way;
- has unlikely, unanticipated or unwanted consequences for individuals;
- creates embarrassment or other negative outcomes, including reputational damage; or
- involves the processing of a wide range of personal data.

Main Establishment

If the controller is conducting cross-border processing, the EDPB guidelines state that it is up to the controller to identify where its main establishment is and therefore which SA will be its lead SA.

Article 4(16) of the GDPR states that 'main establishment' means:

- *As regards a controller with establishments in more than one Member State, the place of its central administration in the [European] 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 [European] 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*[1]
- *as regards a processor with establishments in more than one Member State, the place of its central administration in the [European] Union, or, if the processor has no central administration in the [European] Union, the establishment of the processor in the [European] 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 order to establish where the main establishment is, it is firstly necessary to identify the central administration of the controller in the EU, if any. The approach set out in the GDPR and the revised guidelines is that the central administration in the EU is the place that has the power to make decisions about the purposes and means of processing personal data. However, as is often the case with large multinationals, there may be cases where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity. This means that there can be situations where more than one lead SA can be identified, i.e. in cases where a multinational company has separate decision making centres, in different countries, for different processing activities. However, where a multinational centralises all the power to make decisions relating to the processing of data in only one of its establishments in the EU, then there will only be one SA identified for the multinational.

The EDPB guidelines note that in these situations it will be essential for controllers to identify precisely where the decisions on purpose and means of processing are taken. Correct identification of the main establishment is in the interests of controllers because it provides clarity in terms of which SA they have to deal with in respect of their various compliance duties under the GDPR. These include registering a data protection officer; notifying a risky processing activity or notifying a data security breach.

The EDPB guidelines go on to provide two useful examples to demonstrate the above principles.

Example 1 – centralised processing decisions

A food retailer has its headquarters (i.e. its 'place of central administration') in Rotterdam, Netherlands. It has establishments in various other EU countries, which are in contact with individuals there. All establishments make use of the same software to process consumers' personal data for marketing purposes. All the decisions about the purposes and means of the processing of consumers' personal data for marketing purposes are taken within its Rotterdam headquarters. This means that the company's lead supervisory authority for this cross-border processing activity is the Netherlands supervisory authority.

Example 2 – multi location processing decisions

A bank has its corporate headquarters in Frankfurt, and all its banking processing activities are organised from there, but its insurance department is located in Vienna. If the establishment in Vienna has the power to decide on all insurance data processing activity and to implement these decisions for the whole EU, then as foreseen in Art 4(16) of the GDPR, the Austrian supervisory authority would be the lead authority in respect of the cross border processing of personal data for insurance purposes, and the German authorities (Hessen supervisory authority) would supervise the processing of personal data for banking purposes, wherever the clients are located.

[1] 1 Emphasis added by EDPB in the guidelines.

Identifying the lead SA Groups of Undertakings

Example 2 above is perhaps of more interest as it reflects the assessments many multinationals need to undertake to identify all appropriate lead SAs.

The EDPB guidelines note that where processing is carried out by a group of undertakings that has its headquarters in the EU, the establishment of the undertaking with overall control should be considered to be the main establishment for the group, except where the purposes and means of processing are determined by another establishment. The parent, or operational headquarters of the group of undertakings in the EU, is likely to be the main establishment, because that would be the place of its central administration.

The EDPB is of the view that the reference in the definition to the place of a controller's central administration works well for organisations that have a centralised decision-making headquarters and branch-type structure, i.e. it is clear that the power to make decisions about cross-border data processing, and to have them carried out, lies within the company's headquarters. In such cases, determining the location of the main establishment, and therefore which SA is the lead SA, might be straightforward.

However, the decision system of group of companies could be more complex, giving independent decision-making powers relating to cross border processing to different establishments. In this regard, the EDPB guidelines point out that Recital 36 of the GDPR is useful in clarifying the main factor that shall be used to determine a controller's main establishment if the criterion of the central administration does not apply. This involves identifying where the effective and real exercise of management activities, that determine the main decisions as to the purposes and means of processing through stable arrangements, takes place. Recital 36 also clarifies *that "the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment".*

The following factors are cited as useful for determining the location of this type of controller's main establishment:

- Where are decisions about the purposes and means of the processing given final 'sign off'?
- Where are decisions about business activities that involve data processing made?
- Where does the power to have decisions implemented effectively lie?
- Where is the director (or directors) with overall management responsibility for the cross-border processing located?
- Where is the controller registered as a company, if in a single territory?

The list is not an exhaustive list and other factors may be relevant depending on the controller or processing activity in question. If a SA has reasons to doubt that the establishment identified by the controller is in reality the main establishment for the purposes of the GDPR, it can conduct an investigation into the controller's analysis to determine where the main establishment is located to prevent forum shopping.

Conclusion

Controllers undertaking cross-border processing activities in the EU are required to identify the lead SA that shall have primary responsibility for dealing with those activities. This process may be quite complex in some scenarios (e.g. for groups of companies).

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA