ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 244 rev.01

Guidelines for identifying a controller or processor's lead supervisory authority

Adopted on 13 December 2016
As last Revised and Adopted on 5 April 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Table of Content

1. Identifying a lead supervisory authority: the key concepts. 3
1.1 'Cross-border processing of personal data'. 3
1.1.1 'Substantially affects'. 3
1.2 Lead supervisory authority. 4
1.3 Main establishment. 5
2. Steps to identify the lead supervisory authority 5
2.1 Identify the 'main establishment' for controllers 5
2.1.1 Criteria for identifying a controller's main establishment in cases where it is not the place of its central administration in the EU. 6
2.1.2 Groups of undertakings 7
2.1.3 Joint data controllers 7
2.2 Borderline cases 8
2.3 Processor 9
3. Other relevant issues 9
3.1 The role of the 'supervisory authority concerned' 9
3.2 Local processing. 10
3.3 Companies not established within the EU. 10
ANNEX - Questions to guide the identification of the lead supervisory authority 11

1. Identifying a lead supervisory authority: the key concepts.

1.1 'Cross-border processing of personal data'.

Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data. Article 4(23) of the General Data Protection Regulation (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 Union where the controller or processor is established in more than one Member State; or the*

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

This means that where an organisation has establishments in France and Romania, for example, and the processing of personal data takes place in the context of their activities, then this will constitute cross-border processing.

Alternatively, the organisation may only carry out processing activity in the context of its establishment in France. However, if the activity substantially affects – or is likely to substantially affect - data subjects in France and Romania then this will also constitute cross-border processing.

1.1.1 'Substantially affects'.

The GDPR does not define 'substantially' or 'affects'. The intention of the wording was to ensure that not all processing activity, with *any* effect and that takes place within the context of a single establishment, falls within the definition of 'cross-border processing'.

The most relevant ordinary English meanings of 'substantial' include; 'of ample or considerable amount or size; sizeable, fairly large', or 'having solid worth or value, of real significance; solid; weighty, important' (Oxford English Dictionary).

The most relevant meaning of the verb 'affect' is 'to influence' or 'to make a material impression on'. The related noun -'effect'- means, amongst other things, 'a result' or 'a consequence' (Oxford English Dictionary). This suggests that for data processing to *affect* someone it must have some form of impact on them. Processing that does not have a substantial effect on individuals does not fall within the second part of the definition of 'cross-border processing'. However, it would fall within the first part of the definition where the processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union, where the controller or processor is established in more than one Member State.

Processing can be brought within the second part of the definition if 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'.

The fact that a data processing operation may involve the processing of a number – even a large number – of individuals' personal data, in a number of Member States, does not necessarily mean that the processing has, or is likely to have, a substantial effect. Processing that does not have a substantial effect does not constitute cross-border processing for the purposes of the second part of the definition, regardless of how many individuals it affects.

Supervisory Authorities will interpret 'substantially affects' on a case by case basis. We will take into account 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.

Ultimately, the test of 'substantial effect' is intended to ensure that supervisory authorities are only required to co-operate formally through the GDPR's consistency mechanism *"where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States". (Recital 135)*

1.2 Lead supervisory authority.

Put simply, a 'lead supervisory authority' is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data.

The lead supervisory authority will coordinate any investigation, involving other 'concerned' supervisory authorities.

Identifying the lead supervisory authority depends on determining the location of the controller's 'main establishment' or 'single establishment' in the EU. Article 56 of the GDPR says that:

- *the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the* [cooperation] *procedure provided in Article 60.*

1.3 Main establishment.

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 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;*

- *as regards a processor with establishments in more than one Member State, 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;*

2. Steps to identify the lead supervisory authority

2.1 Identify the 'main establishment' for controllers

In order to establish where the main establishment is, it is firstly necessary to identify the central administration of the data controller in the EU, if any.[1] The approach implied in the GDPR is that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented.

The essence of the lead authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU. In cases where decisions relating to different cross-border processing activities are taken within the EU central administration, there will be a single lead supervisory authority for the various data processing activities carried out by the multinational company. However, 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 authority can be identified, i.e. in cases where a multinational company decides to have separate decision making centres, in different countries, for different processing activities.

It is worth recalling, that where a multinational company centralises all the decisions relating to the purposes and means of processing activities in one of its establishments in the EU (and that establishment has the power to implement such decisions), only one lead supervisory authority will be identified for the multinational.

[1] The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement. The GDPR is currently under scrutiny for incorporation, see http://www.efta.int/eea-lex/32016R0679

In these situations it will be essential for companies 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 and processors because it provides clarity in terms of which supervisory authority they have to deal with in respect of their various compliance duties under the GDPR. These may include, where relevant, designating a data protection officer or consulting for a risky processing activity that the controller cannot mitigate by reasonable means. The relevant provisions of the GDPR are intended to make these compliance tasks manageable.

The examples below illustrate this:

Example 1: 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: A bank has its corporate headquarters in Frankfurt, and all[2] 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. [3]

2.1.1 Criteria for identifying a controller's main establishment in cases where it is not the place of its central administration in the EU.

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".

[2] In the context of processing personal data for banking purposes, we recognise that are many different processing activities involved in this. However, to simplify matters, we address all of them as a single purpose. The same is true of processing done for insurance purposes.

[3] It should be recalled also that the GDPR provides for the possibility of local oversight in specific cases. See Recital (127): *"Each supervisory authority* ***not acting as the lead*** *supervisory authority* ***should be competent to handle local cases*** *where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns* ***only processing carried out in a single Member State and involves only data subjects in that single Member State****, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State."* This principle means that the supervision of HR data connected to local employment context could fall to several supervisory authorities.

The data controller itself identifies where its main establishment is and therefore which supervisory authority is its lead authority. However, this can be challenged by the respective supervisory authority concerned afterwards.

The factors below are useful for determining the location of a controller's main establishment, according to the terms of the GDPR, in cases where it is not the location of its central administration in the EU.

- 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 or processor registered as a company, if in a single territory?

Note that this is not an exhaustive list. Other factors may be relevant depending on the controller or processing activity in question. If a supervisory authority 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 – of course – require the controller to provide the additional information necessary for it to prove where its main establishment is located.

2.1.2 Groups of undertakings

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 is presumed to be the decision-making centre relating to the processing of personal data, and will therefore be considered to be the main establishment for the group, except where decisions about the purposes and means of processing are taken 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 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. In such cases 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 supervisory authority is the lead supervisory authority - is straightforward. However, the decision system of group of companies could be more complex, giving independent making powers relating to cross border processing to different establishments. The criteria set out above should help groups of undertakings to identify their main establishment.

2.1.3 Joint data controllers

The GDPR does not specifically deal with the issue of designating a lead authority where two or more controllers established in the EU jointly determine the purposes and means of processing – i.e. joint controllers. Article 26(1) and Recital 79 make it clear that in joint controller situations, the controllers shall in a transparent manner determine their respective responsibilities for compliance with their obligations under the Regulation. In order, therefore, to benefit from the one-stop-shop principle, the joint controllers should designate

(among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out in the joint controller situation. The arrangement of the joint controllers is without prejudice to the liability rules provided in the GDPR, in particular in Article 82(4).

2.2 Borderline cases

There will be borderline and complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken. This might be the case where there is cross-border processing activity and the controller is established in several Member States, but there is no central administration in the EU and none of the EU establishments are taking decisions about the processing (i.e. decisions are taken exclusively outside of the EU).

In the case above, the company carrying out cross border processing may be keen to be regulated by a lead authority to benefit from the one-stop-shop principle. However, the GDPR does not provide a solution for situations like this. In these circumstances, the company should designate the establishment that has the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets, as its main establishment. If the company does not designate a main establishment in this way, it will not be possible to designate a lead authority. Supervisory authorities will always be able to investigate further where this is appropriate.

The GDPR does not permit 'forum shopping'. If a company claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision making over the processing of personal data takes place there, the relevant supervisory authorities (or ultimately EDPB) will decide which supervisory authority is the 'lead', using objective criteria and looking at the evidence. The process of determining where the main establishment is may require active inquiry and co-operation by the supervisory authorities. Conclusions cannot be based solely on statements by the organisation under review. The burden of proof ultimately falls on controllers and processors to demonstrate to the relevant supervisory authorities where the relevant processing decisions are taken and where there is the power to implement such decisions. Effective records of data processing activity would help both organisations and supervisory authorities to determine the lead authority. The lead supervisory authority, or concerned authorities, can rebut the controller's analysis based on an objective examination of the relevant facts, requesting further information where required.

In some cases the relevant supervisory authorities will ask the controller to provide clear evidence, in line with any EDPB guidelines, of where its main establishment is, or where decisions about a particular data processing activity are taken. This evidence will be given due weight and the supervisory authorities involved will co-operate to decide which one of them will take the lead in investigations. Such cases will only be referred to the EDPB for a decision under Article 65(1)(b) where supervisory authorities have conflicting views in terms of identifying the lead supervisory authority. However, in most cases, we expect that the relevant supervisory authorities will be able to agree a mutually satisfactory course of action.

2.3 Processor

The GDPR also offers the one-stop-shop system for the benefit of data processors that are subject to GDPR and have establishments in more than one Member State.

Article 4(16)(b) of the GDPR states that the processor's main establishment will be the place of the central administration of the processor in the EU or, if there is no central administration in the EU, the establishment in the EU where the main processing (processor) activities take place.

However, according to Recital 36, in cases involving both controller and processor, the competent lead supervisory authority should be the lead supervisory authority for the controller. In this situation, the supervisory authority of the processor will be a 'supervisory authority concerned' and should participate in the cooperation procedure. This rule will only apply where the controller is established in the EU. In cases when controllers are subject to the GDPR on the basis of Art 3(2), they will not be subject to the one-stop-shop mechanism. A processor may provide services to multiple controllers located in different Member States – for example, a large cloud-service provider. In such cases, the lead supervisory authority will be the supervisory authority that is competent to act as lead for the controller. In effect, this means a processor may have to deal with multiple supervisory authorities.

3. Other relevant issues

3.1 The role of the 'supervisory authority concerned'

GDPR Article 4(22) says that the:

> *'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority.*

The concept of a concerned supervisory authority is meant to ensure that the 'lead authority' model does not prevent other supervisory authorities having a say in how a matter is dealt with when, for example, individuals residing outside the lead authority's jurisdiction are substantially affected by a data processing activity. In terms of factor (a) above, the same considerations as for identifying a lead authority apply. Note that in (b) the data subject must merely reside in the Member State in question; he or she does not have to be a citizen of that state. It will generally be easy – in (c) to determine – as a matter of fact – whether a particular supervisory authority has received a complaint.

Article 56, paragraphs (2) and (5) of the GDPR provide for a concerned supervisory authority to take a role in dealing with a case without being the lead supervisory authority. When a lead supervisory authority decides not to handle a case, the concerned supervisory authority that informed the lead shall handle it. This is in accordance with the procedures in Article 61 (Mutual assistance) and Article 62 (Joint operations of supervisory authorities) of the GDPR. This might be the case where a marketing company with its main establishment in Paris launches a product that only affects data subjects residing in Portugal. In such a case the

French and Portuguese supervisory authorities might agree that it is appropriate for the Portuguese supervisory authority to take the lead in dealing with the matter. Supervisory authorities may request that data controllers provide input in terms of clarifying their corporate arrangements. Given that the processing activity has a purely local effect – i.e. on individuals in Portugal – the French and Portuguese supervisory authorities have the discretion to decide which supervisory authority should deal with the matter – in accordance with Recital 127.

The GDPR requires lead and concerned supervisory authorities to co-operate, with due respect for each other's views, to ensure a matter is investigated and resolved to each authority's satisfaction – and with an effective remedy for data subjects. Supervisory authorities should endeavour to reach a mutually acceptable course of action. The formal consistency mechanism should only be invoked where co-operation does not reach a mutually acceptable outcome.

The mutual acceptance of decisions can apply to substantive conclusions, but also to the course of action decided upon, including enforcement activity (e.g. full investigation or an investigation with limited scope). It can also apply to a decision not to handle a case in accordance with GDPR, for example because of a formal policy of prioritisation, or because there are other concerned authorities as described above.

The development of consensus and good will between supervisory authorities is essential to the success of the GDPR's cooperation and consistency process.

3.2 Local processing.

Local data processing activity does not fall within the GDPR's cooperation and consistency provisions. Supervisory authorities will respect each other's competence to deal with local data processing activity on a local basis. Processing carried out by public authorities will always be dealt with on a 'local' basis too.

3.3 Companies not established within the EU.

The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a Member State does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative.

Done in Brussels, on 13 December 2016

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

For the Working Party
The Chairwoman
Isabelle FALQUE-PIERROTIN

ANNEX - Questions to guide the identification of the lead supervisory authority

1. Is the controller or processor carrying out the cross-border processing of personal data?

a. Yes, if:

- the controller or processor is established in more than one Member State and
- the processing of personal data takes place in the context of the activities of establishments in more than one Member State.

➢ In this case, go to section 2.

b. Yes, if:

- the processing of personal data takes place in the context of the activities of a data controller or processor's single establishment in the Union, but:
- substantially affects or is likely to substantially affect individuals in more than one Member State.

➢ In this case, the lead authority is the authority for the controller or processor's single establishment in a single Member State. This must – by logic - be the controller or processor's main establishment because it is its only establishment.

2. How to identify the 'lead supervisory authority'

a. In a case involving only a controller:

i. Identify the controller's place of central administration in the EU;

ii. The supervisory authority of the country where the place of central administration is located is the controller's lead authority.

However:

iii. If decisions on the purposes and means of the processing are taken in another establishment in the EU, and that establishment has the power to implement those decisions, then the lead authority is the one located in the country where this establishment is.

b. In a case involving a controller and a processor:

i. Check if the controller is established in the EU and subject to the one-stop-shop system. If so,

ii. Identify the lead supervisory authority of the controller. This authority will also be the lead supervisory authority for the processor.

iii. The (non-lead) supervisory authority competent for the processor will be a 'concerned authority' – see 3 below.

c. In a case involving only a processor:

i. Identify the processor's place of central administration in the EU;

ii. If the processor has no central administration in the EU, identify the establishment in the EU where the main processing activities of the processor take place.

d. In a case involving joint controllers:

i. Check if the joint controllers are established in the EU.

ii. Designate among the establishments where decisions on the purposes and means of the processing are taken the establishment which has the power to implement these decisions with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out by the joint controllers. The lead authority is the one located in the country where this establishment is.

3. Are there any 'concerned supervisory authorities'?

An authority is a 'concerned authority':

- when the controller or processor has an establishment on its territory, or:
- when data subjects on its territory are substantially affected or likely to be substantially affected by the processing, or:
- when a complaint is received by a particular authority.