Guidance on the General Data Protection Regulation: (2) Lead Supervisory Authority

Guidance Note IR02/17

24th May 2017

Gibraltar Regulatory Authority
Information Rights Division
2nd Floor, Eurotowers 4, 1 Europort Road
Gibraltar
GX11 1AA
Telephone +350 20074636 Fax +350 20072166
Email: privacy@gra.gi
Web: http://www.gra.gi

Contents

Introduction

The General Data Protection Regulation (the "GDPR") will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

This is the second document in a series of Guidance Notes that the Gibraltar Regulatory Authority ("GRA"), as the Data Protection Commissioner, will issue in the run up to the 25th May 2018.

This Guidance Note provides general advice on the Lead Supervisory Authority principle, which is introduced in the GDPR.

Currently, organisations who have establishments in one or more EU Member States may be subject to different data protection laws and enforcement approaches. Going forward, under the GDPR, organisations with several establishments in the EU can benefit from the Lead Supervisory Authority principle and only have to report to one Supervisory Authority i.e. the Lead Supervisory Authority. This is also known as the "one-stop-shop" mechanism, which allows for a more cost-effective approach and is seen as a solution to the problems faced by organisations who operate across multiple EU Member States.

In the following, the GRA provides advice on the GDPR's Lead Supervisory Authority principle.

The Lead Supervisory Authority principle is only relevant where a data controller or data processor is carrying out cross-border processing of personal data.

If your organisation only conducts "local processing of personal data[1]", the Lead Supervisory Authority principle does not apply. The Supervisory Authority you are required to comply with is the Authority in the same jurisdiction your organisation is established and operates in.

1. Cross-border processing

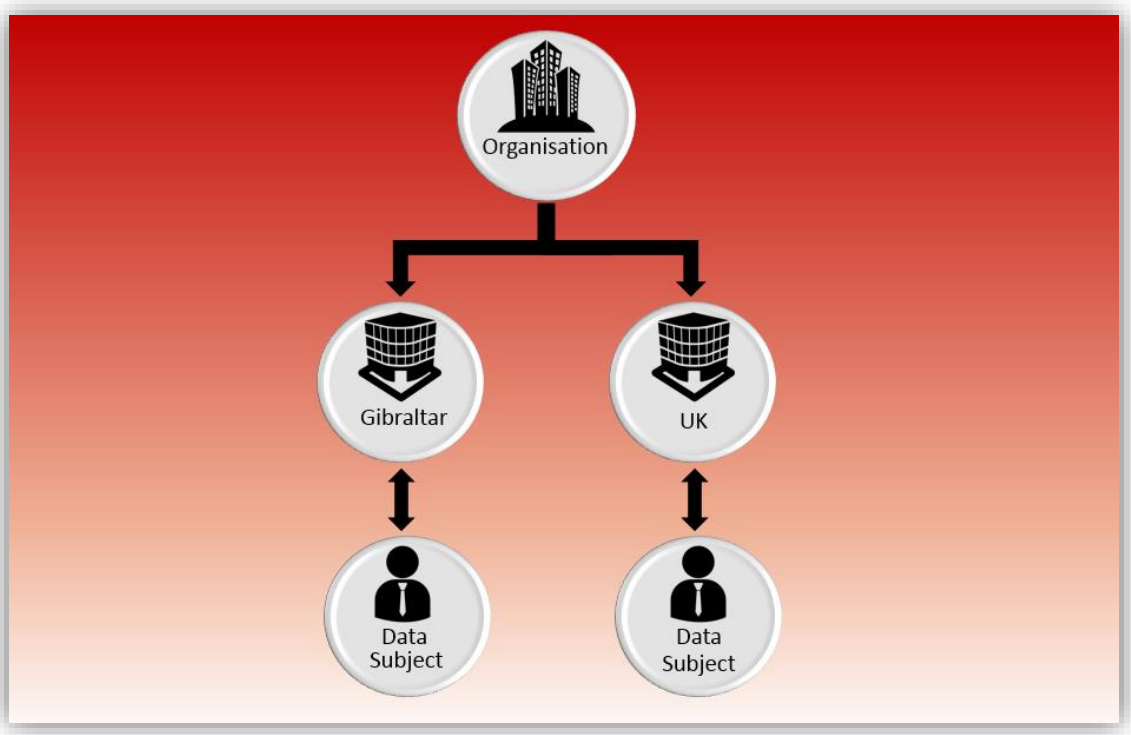
Article 4(23) of the GDPR defines 'cross-border processing' as:

- 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

- 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.

Example 1

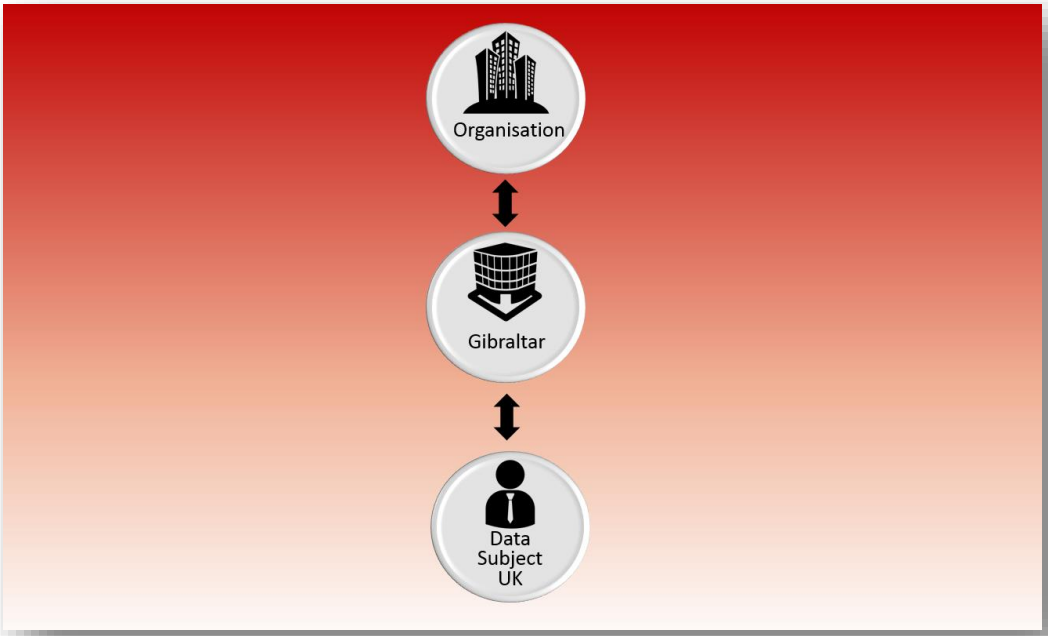
If an organisation has establishments in Gibraltar and the UK, and they both process personal data, then this will constitute cross-border processing.



[1] The processing of personal data about individuals that are "local" to the data controller i.e. within the same jurisdiction. For example, processing carried out by public authorities will most probably always be "local data processing".

Example 2

If an organisation is only established in Gibraltar, but its processing activity substantially affects – or is likely to substantially affect - data subjects in the UK then this will also constitute cross-border processing.



1.1. "Substantially affect"

To trigger the second part of the definition of cross-border processing, the processing of personal data by an establishment in Gibraltar must "substantially affect" (or be likely to) individuals in another EU jurisdiction. The intention of the wording is to ensure that not all processing, with any effect, falls within the definition of cross-border processing.

The GRA will follow the guidance provided by the Article 29 Data Protection Working Party ("WP29"). The WP29 guidance explains that when considering whether a data processing activity will "substantially affect" individuals, what should be taken into account is 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 harm; or
- involves the processing of a wide range of personal data.

2. Lead Supervisory Authority

Once it has been determined that the processing in question is cross-border processing, then the Lead Supervisory Authority must be identified.

According to Article 56 of the GDPR, the Lead Supervisory Authority will be the Supervisory Authority of the main establishment or single establishment (within the EU) of the data controller or processor.

The Lead Supervisory Authority will be the Supervisory Authority with primary responsibility for dealing with cross-border processing, and will for example coordinate any investigation, involving other 'concerned' Supervisory Authorities.

3. Main establishment

In respect of an organisation identifying its 'main establishment', Article 4(16) of the GDPR states that a 'main establishment' means the following:

- 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;

3.1 Identifying the 'main establishment' for data controllers

In summary, the foregoing states that a data controller's main establishment will be –

1) its place of 'central administration' (if any) within the EU, or otherwise
2) the place in the EU where the decisions about the means and purposes of the data processing are made.

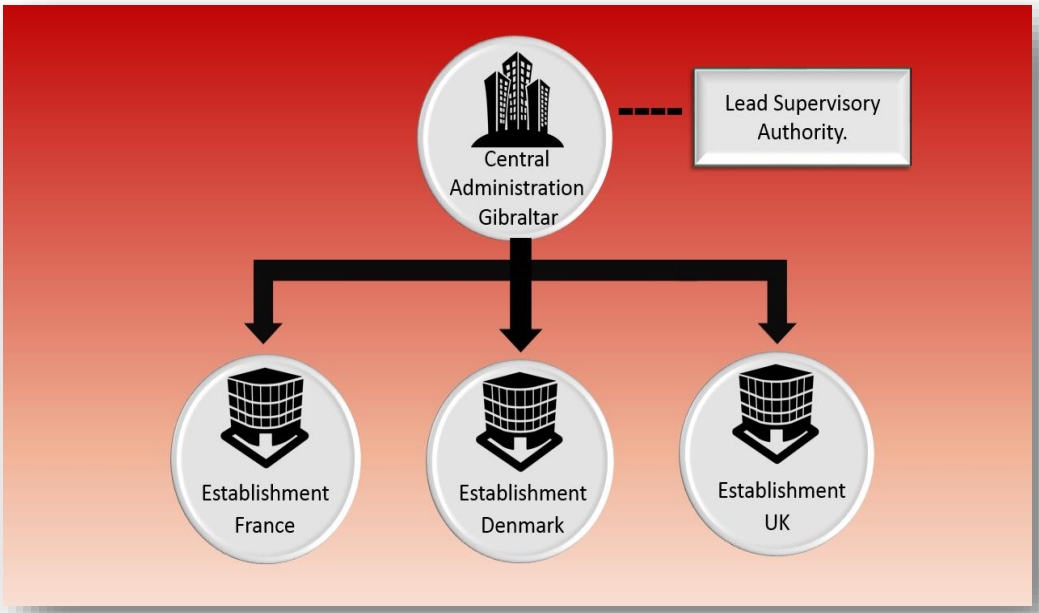
Both scenarios are explained below.

It is important to note, that it is the data controller itself that identifies where its main establishment is and therefore which Supervisory Authority is its Lead Supervisory Authority. However, this can later be challenged by a respective authority concerned.

To identify its main establishment(s), it will be essential for data controllers to identify precisely where the decisions on the purpose and means of processing are taken. Correct identification of the main establishment is in the interest 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 GPDR. This clarity will help make the compliance tasks manageable.

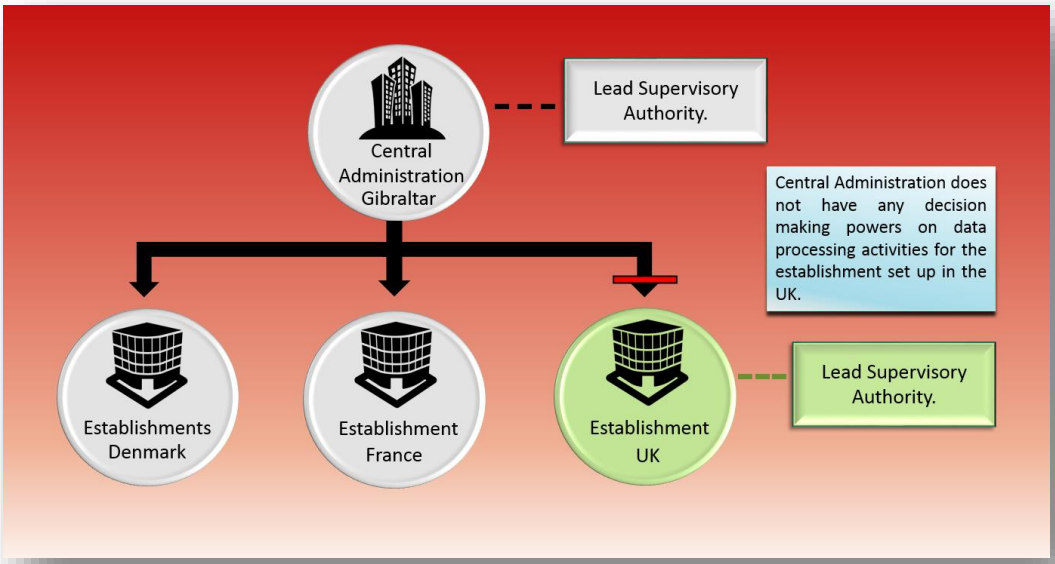
(a) The place of central administration

In cases where a multinational company has several establishments throughout the EU, but decisions relating to the different cross-border processing of personal data by the various establishments are taken within an EU Central Administration, the EU Central Administration will be the organisation's main establishment. In these cases, the Supervisory Authority of the jurisdiction in which the EU Central Administration is located will be the single Lead Supervisory Authority, for the various data processing activities carried out by the group of companies.



(b) The main establishment when it is not the place of central administration

Alternatively, there may be cases where a multinational company decides to have separate decision making centres, in different jurisdictions, for different processing activities. This means that more than one Lead Supervisory Authority can be identified for the various data processing activities carried out by the group of companies.



Further to the above, recital 36 of the GDPR is useful in clarifying the main factor that should be used to identify 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.

According to the WP29, the following list is useful for determining the location of a 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 or processor registered as a company, if in a single territory?

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 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 will decide which Supervisory Authority is the 'lead', using objective criteria and looking at the evidence. The burden of proof ultimately falls on controllers (and processors). They should be able to demonstrate to

Supervisory Authorities where decisions about data processing are actually taken and implemented.

3.2 Identifying the 'main establishment' for Data Processors

Under the GDPR data processors can also benefit from the one stop shop mechanism.

Similarly to data controllers, the GDPR begins by stating that the main establishment shall be its place of central administration within the EU. Otherwise it will be where its main data processor activities take place.

In cases that involve both the data controller and the data processor, the Lead Supervisory Authority shall be that of the data controller, and the Supervisory Authority of the data processor shall be a Supervisory Authority Concerned (see below).

4. Supervisory Authority Concerned

Notwithstanding that the Lead Supervisory Authority has primary responsibility for the regulation of cross-border processing activity, the GDPR allows other Supervisory Authorities to have a say and be involved in the regulation of the cross-border activity. In particular, Supervisory Authorities that are not the Lead Supervisory Authority, can become involved in dealing with a case when –

(a) the controller or processor is established in their jurisdiction;

(b) the data processing substantially affects individuals residing in their jurisdiction; or

(c) they receive a complaint relating to the data processing.

A Supervisory Authority that meets the abovementioned criteria is known under the GDPR as a 'Supervisory Authority Concerned'.

The GDPR requires cooperation between the Lead Supervisory Authority and the Supervisory Authorities Concerned.

5. Organisations outside of the EU

If a company does not have an establishment in the EU then it must deal with Supervisory Authorities in every Member State they are "active" in, through a local representative. The mere presence of a representative in a Member State does not trigger the one stop shop system.

6. Data processing activity in the EU ruled by decision making outside of the EU

There may be cases where a data controller has several establishments throughout the EU, but there is no EU Central Administration and none of the establishments take decisions about the processing activities in the EU (i.e. decisions are taken outside of the EU). In these cases the organisation is unlikely to be able to identify a Lead Supervisory Authority and will likely have to deal with various Supervisory Authorities.

Should an organisation wish to benefit from the one stop shop mechanism, a possible solution would be for the data controller to designate an establishment within the EU that will act as its main establishment. The establishment must have the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets.

Important Note

This document is purely for guidance and aims to supplement the WP29's Guidelines for identifying a controller or processor's Lead Supervisory Authority[2]. The document does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the GDPR will apply directly to them. The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards therefore lies with the organisation.

Where necessary, the GRA will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR, the GDPR will take precedence.

[2] Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (5 April 2017)