

Insights

THE DATA & BREXIT DIGEST – DATA PROTECTION REPRESENTATIVES

WHEN AND HOW TO APPOINT A REPRESENTATIVE FOR THE PURPOSES OF ARTICLE 27

10 March 2021

SUMMARY

With the UK unambiguously out of the EU, this fourth and final instalment of our Data & Brexit Digest explores the topic of appointed representatives under Article 27.

What is an Article 27 representative?

The concept of the Article 27 representative (“**Representative**”) is common to both the UK GDPR and the EU GDPR (the EU General Data Protection Regulation (2016/679)). It is key part of the mechanism by which the territorial reach of the legislation – and its enforcement - is extended beyond the borders of the UK (in the case of the UK GDPR) or beyond the EU (in the case of the EU GDPR).

Under the UK GDPR, a Representative is an individual, company or organisation located in the UK which is “designated in writing” by an entity which lacks a UK presence but which is nevertheless subject to the UK GDPR under Article 3(2). This can happen for example where, as explained below, the appointing entity is targeting the offer of goods or services to individuals who are located in the UK. The obligation to appoint a Representative applies to processor entities as well as controller entities.

A Representative is mandated (usually under a written service contract) to act on behalf of the appointing entity with regard to certain of its obligations under the UK GDPR or EU GDPR as the case may be. In the UK this would primarily involve facilitating communications between a non-UK established entity and the UK’s supervisory authority, the Information Commissioner’s Office (“**ICO**”) or with any affected data subjects in the UK.

Once appointed, an organisation is required to provide data subjects with the identity and contact details of its Representative in accordance with Articles 13 and 14.

When is an organisation required to appoint a UK Representative?

Organisations that are based outside of the UK and which do not have a branch, office or other establishment in the UK are required to comply with UK GDPR in accordance with Article 3(2) where they process personal data in relation to:

- the offering of goods or services to individuals who are located in the UK (in a targeted way),
or
- the monitoring of the behaviour of individuals who are located in the UK.

Complying with the UK GDPR means that such an organisation is required to appoint a Representative in the UK unless the organisation's processing:

- is occasional, i.e. outside the regular course of business or activity of the organisation;
- does not include, on a large scale, processing of special categories of personal data or processing of personal data relating to criminal convictions and offences; and
- is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purpose of the processing.

Public bodies or authorities are not required to appoint a Representative.

The EU GDPR applies a substantially identical set of rules.

What qualities or qualifications does a Representative need?

Representatives, whether based in the UK or the EU, are required to act as a contact point for both data subjects and relevant data protection authorities. Typically Representatives will also play a role in communicating data breach notifications. Representatives are also required to hold and maintain a copy of the record of processing activities ("**ROPA**") of the organisation which appointed them, and to provide it to a supervisory authority on request.

It is recommended that organisations appoint privacy professionals with previous experience in interacting with both supervisory authorities and handling data subject requests. For EU-based Representatives, local language skills are likely to be of importance as they could receive contact from individuals or regulators from a range of countries in that region.

Guidance from the EDPB¹ states that the role of Representative is not compatible with that of Data Protection Officer ("**DPO**") under Article 37 because a Representative is under direct instruction from the appointing entity whereas a DPO requires a level of independence and autonomy within the

organisation. A Representative therefore cannot also serve as the DPO. In addition, the EDPB recommends that a processor appointed by an organisation should not also serve as its Representative in order to avoid any possible conflicts of interest or obligation in cases of enforcement. This guidance is not binding in the UK but is likely to be influential on the ICO.

Designating a Representative does not affect the responsibility or liability of the appointing entity for its own data protection breaches or failings. The Representative does have some direct responsibilities under the legislation however these are fairly narrow under the UK GDPR and limited to matters related to the ROPA (Article 30) and other information ordered to be provided by the ICO (Article 58(1)(a)).

Where should they be located?

Under the UK GDPR, the Representative should of course be in the UK.

Under the EU GDPR, this is more nuanced. A Representative should be located in one of the EU Member State where individuals whose personal data are being processed, are also located. When selecting the location (and qualities), an organisation will want to ensure that the Representative is in a position to communicate efficiently with supervisory authorities and data subjects.

Brexit and the need to appoint a Representative

The end of the Brexit transition period on 31 December 2020 triggered the following potential changes in terms of the obligation to appoint a Representative for affected organisations:

- Companies outside the UK which are subject to the UK GDPR need to appoint a UK Representative; and
- Companies in the UK (with no EU branch, office or other establishment) which are subject to the EU GDPR need to appoint an EU Representative.

The UK's data protection regime looks set for a period of change in 2021, notwithstanding the significant impact already brought about by Brexit. Businesses with UK operations or customers will need to be alert to these regulatory changes and monitor developments carefully.

This briefing is not legal advice. Please feel free to contact any team member if you would like to discuss any of the issues covered in this instalment.

1. Guidelines 3/2018 on the territorial scope of the GDPR, version 2.0, 12 November 2019.

RELATED CAPABILITIES

- Data Privacy & Security

- General Data Protection Regulation
- Regulation, Compliance & Advisory

MEET THE TEAM



Geraldine Scali

Co-Author, London

geraldine.scali@bclplaw.com

[+44 \(0\) 20 3400 4483](tel:+442034004483)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.