

SHOOSMITHS

The legal requirement for a UK Representative

The background to the UK Representative requirement

- The General Data Protection Regulation (“GDPR”) came into force in May 2018. This contains a law specifically designed to extend the scope of the GDPR to companies which are based outside the EU, but which target or monitor EU individuals and process their data in doing so. This law was considered necessary to address the huge increase in e-commerce, online monitoring and data analytics of EU-based individuals by businesses outside the EU. This is the so-called “extra-territorial provision”, and is contained in Article 3(2) of the GDPR.
- Most businesses that are caught by Article 3(2) must also appoint a representative in the EU. The reasoning for this is that both the data protection regulators in the EU (known as “supervisory authorities”) and EU-based individuals whose data is being processed (known as “data subjects”) should have a local point of contact, to whom they may address their enquiries, requests and investigations. The requirement to appoint a representative is contained in Article 27 of the GDPR.
- Following Brexit, the United Kingdom government wishes to ensure that its own data protection laws remain aligned to the GDPR for the foreseeable future. With this in mind, the UK Parliament has passed a regulation which creates a UK version of the GDPR, known as “UK GDPR”. This is almost identical to the GDPR, except that references to the EU are replaced with references to the UK.
- The UK GDPR comes into effect at 11:00 pm (UK local time) on 31 December 2020, when the transitional arrangements between the UK and the EU come to an end.
- Note that the requirement to appoint a UK representative is unaffected by the question of whether (and when) the EU Commission officially decides that the UK’s domestic laws provide an adequate level of protection for EU data subjects, which is known as an “adequacy decision”. Currently only a handful of non-EU countries around the world have been found to be “adequate” by the EU, and the process typically takes a considerable period of time. It is expected that the UK will receive an adequacy decision at some point, but in our view this decision will reinforce, rather than undermine, the need for protections such as the requirement to appoint a UK representative.

“both the regulators, and EU-based individuals whose data is being processed, should have a local point of contact”

What businesses are required to appoint a UK Representative?

Under the UK GDPR, a business must appoint a UK Representative in the following circumstances:

- the business has no UK footprint – in other words, it is not established in the UK, e.g. by having an office, branch or group company;
- the business processes personal data of UK data subjects. The concepts of ‘personal data’, ‘processing’ and ‘data subjects’ are very wide, and any collection, storage, analysis or other use of any personal information relating to UK individuals is very likely to be caught. (Please see the glossary on page 4 for further details.)
 - the processing either
 - relates to the targeted offering of goods or services to the UK data subjects. Both paid-for and free-of-charge goods or services are covered. Merely operating a website which UK individuals can visit is not by itself enough – the test is whether there is some kind of targeted marketing or offering directed to the UK.
 - or relates to the monitoring of their behaviour in the UK. This would typically (but not always) involve online monitoring or data analytics.

Note that this requirement covers both “controllers” and “processors” of the personal data (see the glossary below for further details). In other words, it would cover both (a) a business which markets or sells into the UK for its own purposes and decides why and how personal data is used for those activities – acting as a ‘controller’ - and (b) a service provider or vendor to that business which provides back-office functions (e.g. hosted CRM, accounting, data analytics) and is purely processing on behalf of that business – acting as a ‘processor’.

- the processing is not exempted. There is a limited exception to the requirement for a UK representative where the processing in question is (a) occasional, and (b) does not include processing on a large scale of ‘special categories’ of data (including health and biometric data, and data relating to religion and ethnic origin – see the glossary below for a full list), or data relating to criminal convictions or offences, and (c) it is unlikely to risk the essential privacy rights of UK individuals. The purpose of this exemption is to ensure that a business does not need to appoint a UK representative if it only occasionally processes data and the nature of that processing does not create any significant risks.
- the business is not a public authority or body. So non-UK government bodies or agencies do not need to appoint UK representatives.

In practice this means that all private sector businesses, which have no UK footprint but which frequently process data of UK individuals, will need to appoint a UK representative, if their processing relates to the targeted offering of goods or services to those individuals, or relates to the monitoring of their behaviour of those individuals in the UK.

Businesses must appoint a UK representative by no later than 11pm (UK time) on 31 December 2020.

“the processing must either relate to the targeted offering of goods or services to UK data subjects, or relate to the monitoring of their behaviour in the UK”

What are the consequences of a failure to appoint a UK representative?

The UK GDPR empowers the UK data protection regulator, the Information Commissioner's Office (ICO) to launch investigations and ultimately to impose significant fines against the business for a failure to appoint a UK representative. The maximum fines which can be imposed are whichever is the higher of:

- 2% of the total worldwide annual turnover of the business in the preceding financial year; or
- £8.7 million.

What is the role of the UK representative?

The core responsibilities of the UK representative are as follows:

- to act as point of contact in the UK with the Information Commissioner's Office (ICO), and all UK data subjects of the business. Note that the underlying obligations (e.g. to delete or correct personal data, or to provide information on what information is held about an individual) remain with the business.
- to maintain a copy of the 'Record of Processing Activities' of the business. This is a core record summarising:
 - the categories of data subjects,
 - the categories of personal data processed,
 - the purposes of processing,
 - how long the data is held for,
 - what other companies will have access to the data or receive copies of it,
 - which countries the data will be transferred to, and what safeguards are in place to protect the rights of data subjects in those countries, and
 - the security measures deployed in the business to prevent data loss or breaches.

Also, where a business is processing personal data in the course of providing a service to its own clients (and on behalf of those clients), it must also list those clients.

Note that the business itself must keep the master version of the Record of Processing Activities, and ensure it is always up to date, and the UK representative keeps a copy of that. There is an exemption for businesses which employ fewer than 250 people. In this case, neither the business nor the UK Representative need to have a Record of Processing Activities, unless the processing represents a higher risk to individuals (e.g. it involves 'special categories' of personal data or criminal conviction or offence data) or is performed frequently.

to disclose a copy of the 'Record of Processing Activities' to the ICO, if requested. Note that the Record of Processing Activities is not a public document and would remain private and confidential document, even if it is required to be disclosed to the ICO.

- to co-operate with the ICO generally in relation to any requests, notices, orders or investigations.

“core responsibilities are to act as point of contact in the UK, and to maintain a copy of the ‘Record of Processing Activities’”

Glossary

- **“controller”**: any person or entity which, alone or jointly with others, determines the purposes and means of the processing of personal data **“data subject”**: an identified or identifiable (living) individual, who is the subject of personal data
- **“personal data”**: means any information relating to a data subject. This covers any information which enables a person to be identified, directly or indirectly, or which relates to that person. The concept is very wide and in particular covers factors such as name, contact details, location data, online identifiers. It also includes biographical details including financial, physical, economic, cultural and social information about the individual. Certain defined types of personal data known as ‘special categories of data’ attract higher protection (see below)
- **“processor”**: any person or entity which processes personal data on behalf of a controller
- **“processing”**: covers any action relating to personal data, including collection, storage, analysis, transfer and deletion
- **“special categories of data”**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic, biometric and health data; data concerning sex life or sexual orientation.

Contact:

To find out more, email us at: contactus@dataprivacyrep.com

DISCLAIMER

This information is for educational purposes only and does not constitute legal advice. It is recommended that specific professional advice is sought before acting on any of the information given.

©Shoosmiths LLP 2023

SHOOSMITHS

www.shoosmiths.com

**FOR
WHAT
MATTERS**