October 2018

Brexit, your business and data: processing European personal data

And so we wait. Theresa May battles on with negotiations but although she assures us that 95% of the deal is done, UK businesses are no closer to certainty around planning for their future.

One of the many issues facing UK businesses is their ability to continue to process personal data about European Union (**EU**) citizens. Following our recent briefing on the impact of a 'no deal' on data transfers in and out of the UK, we continue to explore the implications of Brexit for UK businesses and their ongoing compliance with data protection law.

In this briefing, we consider how UK businesses which conduct cross-border trading in the EU will be affected by the General Data Protection Regulation (2016/679) (**GDPR**) as it applies in the EU (and the European Economic Area (**EEA**), by virtue of its incorporation into the EEA Agreement), when the UK becomes a "third country" (i.e. a country outside of the EEA) following Brexit. In particular, we look at how (insofar as they process data about EU data subjects) UK businesses will need to:

- adjust to having a new data protection regulator in place of the ICO (in respect of their EU activities); and in some cases
- appoint a representative in the EU.

The first point will not come as a surprise – businesses trading overseas, particularly when consumer facing, regularly need to decide how far to mould their trading operations around complying with local law to the letter, or whether to take the risk of a "one size fits all" approach, which is already the case with GDPR. The second point will be new to UK businesses. In this briefing, we aim to not only inform you of the issues, but also draw your attention to the practical steps you should think about now.

Territorial application

As we saw in our last briefing, upon Brexit, GDPR will continue to apply in the UK to the processing of personal data about UK data subjects. But following B(rexit)-Day, the UK will cease to be a member of the EU, and will become a "third country" for EU purposes. As such, how UK businesses have to comply with GDPR as it applies in the EU raises issues which are additional to those faced in complying with GDPR as it is applied in the UK.

Following B-Day, in addition to complying with GDPR in domestic law, UK businesses will need to comply with GDPR as it applies in the EU, if:

- they have an establishment within the EU and process personal data about EU data subjects; or
- without having an establishment in the EU, they process personal data about data subjects who are in the EU and the processing activities are related to either the:
  - **a.** offering of goods or services to such data subjects in the Union; or
  - **b.** the monitoring of their behaviour (as far as their behaviour takes place within the EU).

This does not affect group companies incorporated in other EU Member States, which will remain subject to GDPR in their own right.

Of course UK businesses trading in other Member States already need to comply with GDPR as interpreted under two (or more) separate systems of law, as GDPR allows local derogations in Member States, and variances will exist. However, the UK has traditionally adopted a high standard of data protection in comparison to the other Member States. So in practice, there may not be many instances where UK businesses will need to adapt their operations to be in line with different data protection standards in the EU. Therefore this shouldn't, in theory, be a major problem.

No more "one stop shop"?

However, Brexit has thrown a spanner in the works when it comes to coordinating EU operations via the GDPR's "one stop shop" (OSS) principle, which would normally have been a handy way of dealing with deviances in approach to data protection amongst the Member States.

Currently under the GDPR, UK businesses benefit from the OSS principle, which allows a single data protection authority (which for UK businesses is most likely the ICO) to be designated as the lead supervisory authority (**LSA**) for organisations carrying out cross-border processing. Businesses that currently benefit from this mechanism are able to use the ICO as their sole interlocutor, to coordinate actions and complaints regarding cross-border processing (e.g. a complaint originating in France or Germany), with the help of other "concerned DPAs" (i.e. other data protection authorities in Member States affected by the processing).

To rely on this principle, the relevant business must demonstrate that it has a "main establishment" (or "single establishment") in the jurisdiction of the LSA. According to Article 29 Working Party guidance (adopted by the replacement European Data Protection Board (**EDPB**)), the "main" or "single" establishment of a business will generally be the place of central administration, which is the place where decisions about the purposes and means of personal data processing are taken. For many UK businesses this is based in the UK.

The difficulty, is that, following B-Day when the UK becomes a third country, the ICO can no longer be a supervisory authority for EU GDPR purposes. For a UK business (or indeed any business which has to date "appointed" the ICO as its LSA) to be able to continue to benefit from the OSS principle in the EU, it will need to appoint a LSA in an EU Member State, but it can only do so if it can show that it has a "main establishment" in that state.

If a business is part of a wider group, with other group companies or undertakings in the EU, which play a meaningful role in decisions about data processing, it may well be able to demonstrate this. The EDPB guidance suggests that in borderline cases entities which make decisions about the purposes and means of data processing, which can assume liability for such processing, and which have sufficient assets to meet the potential sanctions, could qualify for "main establishment" status.

Representatives of controllers and processors based in "third countries"

Even if a UK business has no establishment within the EU, the GDPR can still, in the instances set out earlier in this briefing, apply. If so, a new requirement for such businesses is that they will have to appoint a representative in the EU, in one of the countries where affected EU citizens live.

The representative will be the primary point of contact for UK businesses for cooperating and communicating effectively with supervisory authorities and data subjects on issues of data processing, for the purposes of ensuring compliance with the organisation's obligations under the GDPR. Accordingly the representative must be designated in writing by the business, and mandated to be addressed in addition to, or instead of, that business. Consequently, you should only appoint someone you would trust to pass on communications to you promptly – traditionally businesses have appointed a fellow group company in comparable situations, but this won't be feasible for everyone.

Failure to appoint a representative pursuant to GDPR could result in a fine up to the greater of €10 million or 2% of global turnover. So this should definitely make it onto the list of Brexit action points for UK businesses.

So what should you do to prepare?

UK businesses which process data about EU data subjects should consider the following steps in preparation for Brexit:

- **Consider checking for material variances in interpretation of the GDPR** in those Member States where your data subjects reside (for example, variances in data breach notification requirements or requirements to appoint a data protection officer), to avoid the risk of falling foul of EU practices or interpretations which differ from those of the

UK. Any such variances should be worked into your business' approach to data protection compliance, such as (amongst other things), addressing any differences in your business' internal response and privacy policies.

- **Consider if you are still able to benefit from the OSS principle/consider whether this is something which is particularly desirable for your businesses.** If it is, and to the extent that you are able to influence the situation, do you have a particular LSA in mind? In order to benefit, you'll need to show that you have a "main" or "single" establishment in the particular Member State of the LSA (see table below).

- **Appoint an EU representative** if you do not have an establishment in the EU – and update your Article 13/14 privacy notices so that they set out the identity and contact details of your representative.

"MAIN" OR "SINGLE" ESTABLISHMENT – CAN YOU MAKE THE ONE STOP SHOP (OSS) WORK FOR YOU?

The table below sets out a few scenarios affecting UK businesses on Brexit. It is a simplified summary of the guidance issued by regulators to indicate what constitutes a "main" or "single" establishment, and the circumstances in which an LSA can validly be nominated, so if this issue is relevant to you it will only serve as a starting point for further analysis – and in any event where you nominate an LSA it will be important to ensure that you appropriately document the reality of how you run the business, in order to demonstrate to the LSA that relevant tests are met.

Scenario	Can the OSS apply?
"I sell direct into the EU from the UK"	**No** – the OSS does not apply where there is no "establishment" within the EU. Having a representative (as is required) doesn't count.
"I sell into the EU via my branch in (e.g.) Germany"	**Yes** - this will be a "single" establishment and Germany is LSA, **provided** that decisions about processing personal data are demonstrably made by the branch. If they aren't (e.g. because decisions are made in the UK), or it isn't clear, you can bring the branch within the OSS mechanism by ensuring that the branch can make the decision on the purpose and means of processing, suitably documenting this.
"I sell into the EU via my group company in (e.g.) Germany"	**Yes** – this will be the "single" establishment and Germany is LSA, **provided** that decisions about processing personal data are demonstrably made by the group company – as with the branch example above.
"I sell into the EU via branches and/or group companies in (e.g.) France, Italy and Spain"	**Yes** – you can use as LSA the supervisory authority in the territory of one of your branches/group companies **provided** that (as with the examples above relating to "single" establishments) decisions about processing personal data (for the whole of the EU) are demonstrably made by the branch or group company within the territory of the LSA nominated by you. This branch/group company will then be the "main establishment". While GDPR does not allow "forum shopping" to nominate the LSA you prefer, it may be possible to restructure your decision making structures to demonstrate that a particular branch/group company is the "main establishment" – but in order to convince the supervisory authorities, this will need real substance. Different business streams may have different "main establishments" (and therefore different LSAs) e.g. a bank which carries on banking and insurance activities from different locations.
"I sell into the EU via branches and/or group companies in (e.g.) France, Italy and Spain, but all decision making happens in the UK.	**No** – there won't be a "main establishment "for OSS purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Dan Reavill
Head of Commercial, IP & Technology

E: dan.reavill@traverssmith.com
T: +44 (0)20 7295 3260

Louisa Chambers
Partner, Commercial, IP & Technology

E: louisa.chambers@traverssmith.com
T: +44 (0)20 7295 3344

James Longster
Partner, Commercial, IP & Technology

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496

Anita Sivapalan
Associate, Commercial, IP & Technology

E: anita.sivapalan @traverssmith.com
T: +44 (0)20 7295 3720