Brexit's Implications for Data Protection in 8 Questions

INTRODUCTION

The UK is set to leave the EU on 31 January 2020. As the EU and the UK prepare for Brexit, companies should too. Brexit continues to raise many legal questions and uncertainties, not the least for the protection of personal data which flows between the UK and the rest of Europe. Will organisations in the UK still have to comply with the General Data Protection Regulation (**GDPR**)?[1] Can they still transfer personal data to the EU? Will they need to appoint a representative in the EU? And what will happen with the one-stop-shop?

What needs to be done will depend on whether a withdrawal agreement will be concluded and on the content of that agreement. However, organisations cannot afford to wait until all the details of Brexit are cast in stone. Instead, they should start preparing now in order to be ready to implement necessary measures as soon as the details of Brexit are sorted out.

On the basis of eight frequently asked questions, we provide an overview of issues to consider and steps to take to start preparing now in order to be ready for Brexit.

1. WILL THE GDPR CONTINUE TO APPLY AFTER BREXIT?
2. WILL I BE ALLOWED TO CONTINUE TRANSFERING PERSONAL DATA FROM THE EU TO THE UK AND VICE VERSA?
3. WILL I HAVE TO APPOINT A EUROPEAN OR UK REPRESENTATIVE?
4. I AM BASED IN THE UK BUT HAVE OFFICES, BRANCHES OR OTHER ESTABLISHMENTS IN THE EU: WHO WILL BE MY LEAD SUPERVISORY AUTHORITY?
5. DO I NEED TO APPOINT A NEW DATA PROTECTION OFFICER?
6. WHERE DO I NOTIFY DATA BREACHES AFTER BREXIT?
7. WILL THE PROTECTION OFFERED BY THE EU AND UK DATA PROTECTION RULES REMAIN THE SAME?
8. SHOULD I START PREPARING NOW OR CAN I WAIT UNTIL BREXIT IS ACTUALLY THERE?

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1 | WILL THE GDPR CONTINUE TO APPLY AFTER BREXIT?

For any organisation that is established in the EU27 (*i.e.*, the EU without the UK), the organisation will have to continue to comply with the GDPR for all activities in the context of such establishment.

Even if your sole EU establishment is currently located in the UK, the GDPR could still apply after Brexit. The short-term response depends on whether the UK will leave the EU with or without a deal. The current draft Withdrawal Agreement foresees the application of EU data protection law until 31 December 2020 (with a possible extension of the transition period for up to two years).[3] Moreover, it provides that EU data protection rules will continue to apply to personal data of data subjects outside the UK that were processed under EU rules before the end of the transition period, unless the UK were to receive an adequacy decision (see, Question 2).

Deal or no deal, if you are not established in the EU, the GDPR in any case applies extraterritorially to the processing of personal data to "target" individuals in the EU by (i) offering goods or services to individuals in the EU ("targeting by selling"); or (ii) monitoring the behaviour of individuals in the EU ("targeting by monitoring"). The latter implies that the controller (*i.e.*, the organisation that determines the purpose and means for the processing) has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU (*e.g.*, behavioural advertisement or online tracking through the use of cookies).

Moreover, the UK Government has expressed its intention to adopt its own version of the GDPR (the so-called *UK GDPR*). Data protection obligations will therefore remain very similar after Brexit for organisations based in the UK (however, see Question 7).

3 Article 132 of the Draft Agreement on the Withdrawal of the United Kingdom from the European Union, published on 17 October 2019, available here.
4 The UK GDPR would have extraterritorial implications similar to the GDPR and may therefore also become relevant for controllers and processors established outside the UK.

2| WILL I BE ALLOWED TO CONTINUE TRANSFERRING PERSONAL DATA FROM THE EU TO THE UK AND VICE VERSA?

In principle, transfers of personal data between the EU and the UK will no longer be unrestricted once the UK becomes a third country.

A framework of protection needs to be implemented to transfer data from the EU to the UK. The GDPR foresees the possibility for the European Commission to adopt an "adequacy decision". With such a decision for the UK, the European Commission recognises that the UK legislation ensures a high level of data protection that is at least similar to the GDPR. Since the adequacy decision procedure can only be initiated officially once the UK becomes a third country, and since the procedure usually takes quite some time, companies should consider implementing other appropriate safeguards in the meantime.[5]

For most organisations these appropriate safeguards will take the form of Standard Contractual Clauses (**SCC**). The SCC are a contractual arrangement that offers adequate safeguards with respect to the protection of personal data when it is transferred to a third country.[6] Alternatively, some organisations may wish to rely on Binding Corporate Rules (**BCR**) that authorise international transfers within the same group of companies.

BCR are binding policies on the protection of personal data that must be approved by the data protection authority of the company's lead supervisory authority. The approval process usually takes several months, so BCR may not provide a short-term solution if the approval process has not yet been initiated. In addition, if you have BCR in place, these will need to be updated to recognise the UK as a third country.

A third alternative provided by the GDPR is to adhere to codes of conduct that are approved by the European Data Protection Board (**EDPB**) or adhere to other clauses that would be approved. However, such measures are currently not yet available and therefore will not provide a short-term solution on Brexit day.

Only in case of exceptional circumstances and if the transfer is not structural, massive or repeated, can you transfer personal data outside the EU without any of the above-mentioned safeguards. In such specific or exceptional situations, international transfers may be permitted on the basis of a data subject's informed and explicit consent, if it is necessary to defend a legal claim, or on the basis of other derogations set out in Article 49 of the GDPR.

For data transfers from the UK to the EU, the UK Government has confirmed that, after Brexit, such data transfers will not be restricted. They will be covered by transitional provisions pending a UK adequacy decision. Even if the UK failed to adopt such an adequacy decision recognising the EU, the UK GDPR will most likely require similar safeguards as set out above.

5 The Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom (2019/C 384 I/02, available here), sets out that the European Commission will initiate an adequacy review "*as soon as possible after the United Kingdom's withdrawal*", in order to adopt an adequacy decision by the end of 2020. The UK will in the same timeframe take steps to allow transfers of personal data from the UK to the EU.

6 Please note that the validity of the SCC is currently under review by the Court of Justice of the EU. This will need to be taken into account when opting for the appropriate transfer mechanism.

3 | WILL I HAVE TO APPOINT A EUROPEAN OR UK REPRESENTATIVE?

If you are based outside the EU (and do not have any offices, branches or other establishments in the EU) the GDPR may nevertheless apply to your organisation if you "target" data subjects in the EU (see, Question 3). In such a case, the GDPR requires that a representative in the EU is designated. The representative – set up in the Member State (or one of the Member States) where the data subjects are located that are monitored, or to whom goods or services are offered – acts on behalf of the controller or processor with regard to their obligations under the GDPR and is the direct point of contact for data subjects and the competent authorities. You must provide the data subjects with the details of the representative, which are usually mentioned in the privacy notice.

Under the UK GDPR, the UK Government intends to require a controller or processor not established in the UK to appoint a UK representative under the same conditions as described above.

***EXCEPTION:** The requirement to appoint a representative does not apply to (i) public authorities; and (ii) occasional processing activities with a low risk for the protection of rights and freedoms of individuals which does not involve the large-scale use of special category or criminal offence data.*

4 | I AM BASED IN THE UK BUT HAVE OFFICES, BRANCHES OR OTHER ESTABLISHMENTS IN THE EU: WHO WILL BE MY LEAD SUPERVISORY AUTHORITY?

The GDPR introduced a "one-stop-shop" mechanism, meaning that, in principle, a company only has to deal with a (single) lead supervisory authority if it is carrying out cross-border personal data processing activities. This mechanism thus establishes a single point of contact and precludes your organisation having to deal with questions from various authorities in parallel. The lead supervisory authority acts on behalf of the other EU supervisory authorities and is responsible for regulating your cross-border processing and for enforcing the GDPR (including by issuing fines).

As an organisation, you should therefore consider whether, following Brexit, you can still benefit from a lead supervisory authority in the EU. If the ICO is currently your lead supervisory authority, you may need to designate a new lead supervisory authority. The lead supervisory authority is the authority of the Member State where the main establishment or single establishment in the EU is located. To benefit from the one-stop-shop it may be required to transfer the decision making on the protection of personal data to the location of the "main" establishment in the EU.

5 | DO I NEED TO APPOINT A NEW DATA PROTECTION OFFICER?

The Data Protection Officer (DPO)

Some data controllers and data processors are required by the GDPR to designate a DPO. This obligation applies if (i) you are a public authority or body; (ii) your core activities require large scale, regular and systematic monitoring of individuals; or (iii) your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences. Groups of undertakings can designate one DPO for the entire group provided that the DPO is easily accessible from every establishment and for all the data subjects concerned.

Even if the GDPR does not require the DPO to be located within the EU, the Article 29 Working Party recommends this, whether or not the controller or the processor is established in the EU.

If you currently appointed a DPO in the UK for a group of undertakings, the same person can continue to act as DPO after Brexit. However, you should assess whether the DPO is easily accessible from the EU.

6 | WHERE DO I NOTIFY DATA BREACHES AFTER BREXIT?

Under the GDPR, the controller must notify personal data breaches to the supervisory authority within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. After Brexit, some UK organisations may still be subject to the GDPR if they have an establishment in the EU or if they target EU data subjects (see, Question 1). The duty to notify a personal data breach under the GDPR may therefore still apply to you.

It is important to consider which supervisory authority must be notified. This will depend on whether the UK organisation has an establishment in the EU or not.

If you have an EU establishment, any local breaches must be notified to the local supervisory authority and breaches of a cross-border processing must (only) be notified to your lead supervisory authority, *i.e.* the authority of the Member State where you have your single or main EU establishment. If you do not have an EU establishment, you should notify cross-border breaches to the supervisory authority of the Member State where your EU representative is located (see, Question 3).

Under the UK GDPR, EU companies will have a similar duty, subject to the same conditions, to notify personal data breaches to ICO.

CYBER SECURITY

How Will I Protect Network and Information Systems After Brexit?

The *Directive concerning measures for a high common level of security of network and information systems across the Union (***NIS Directive***)* creates common standards on network and information security across the EU for *"operators of essential services"* (*i.e.*, operators in the health, water, energy, transport, digital and financial sectors) and for *"digital service providers"* (*i.e.*, online marketplaces, search engines and cloud computing services).[7] As it is a Directive, the national laws implementing the NIS Directive will continue to apply after Brexit.

The NIS Directive requires digital service providers not established in the EU to appoint an EU representative in the Member State (or one of the Member States) where the services are offered. To determine whether you offer services in the EU that fall under the NIS Directive, factors such as the use of a language or currency generally used in a Member State or the mentioning of customers or users located in the EU will play a role, among other factors. You will need to comply with the domestic legislation implementing the NIS Directive in that Member State where services are offered.

The NIS Directive imposes obligations with regard to preventive network and information security requirements. In addition, organisations within the material scope of the NIS rules must notify incidents with a substantial impact on the provision of services to the national authorities of that Member State. If the incident also relates to personal data, the notification under the NIS Directive comes on top of the data breach notification obligation under the GDPR. Accordingly, organisations should ensure that their incident response plans provide clear triggers to notify all relevant authorities in case of a breach.

7 | WILL THE PROTECTION OFFERED BY THE EU AND UK DATA PROTECTION RULES REMAIN THE SAME?

The UK Government intends to write the GDPR into UK law, resulting in a "UK GDPR". Therefore, in the short to medium term at least, the regulatory regimes for personal data protection will remain the same or at least very similar. However, the rules may diverge over time, either because the EU or UK amends its data protection rules, or as a consequence of UK regulators no longer being bound by interpretations of the Court of Justice of the EU (**CJEU**) or the European Data Protection Board (**EDPB**). Indeed, escaping the CJEU's jurisdiction is one of the reasons why the UK wishes to leave the EU. Instead, the UK Supreme Court will be the ultimate interpreter of the UK GDPR and ICO will publish its own guidance on the interpretation and application of data protection rules in the UK.

It is therefore possible that, after some time, equivalent rules should be applied differently depending on their interpretation in the EU or UK. Such differences may also be relevant if the UK were to receive an adequacy decision of the European Commission (see, Question 2), as this decision will need to be reviewed on a regular basis. Such review will look at possible divergences between EU and UK data protection rules. If the divergence were to become significant, the adequacy decision could be revoked.

7 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *EU OJ* L 194, p. 1. This Directive has been transposed into UK law by the NIS Regulations (SI 2018/506).

8 | SHOULD I START PREPARING NOW OR CAN I WAIT UNTIL BREXIT IS ACTUALLY THERE?

The above questions show that Brexit is likely to raise some data protection issues. For some of these issues, the exact requirements that you must take will need to be determined depending on whether there will be a "deal" or "no deal" Brexit. While supervisory authorities could announce a grace period for implementing the measures that are required after the details of how Brexit will be organised become clear, they are unlikely to be very forgiving for organisations that failed to take preparatory measures seeing that Brexit-related topics have dominated news headlines for the past three years. Indeed, the GDPR already requires organisations to be "accountable" and accountability includes having a clear plan for protecting personal data after Brexit. Below, we provide an outline of what such a plan should cover.

TO DO:

Start mapping your data flows (if any) between the EU and the UK and have a clear view on contracts relating to such data flows. Mapping data flows may take some time, so it should not be left until the last minute.

Set out your strategy for international transfers outside the EU: do you opt for SCC or BCR? In the latter case, you may already have to start implementing the BCRs. A clear strategy will be needed in order to act fast once the details of Brexit are known.

Review your current contracts, including data processing agreements, general terms and conditions and other contracts with data protection clauses. The wording of these clauses may need to be updated to reflect the new situation after Brexit. For instance, if your contract asserts that personal data will not be transferred outside the EU, but you store data in the UK, you may need to amend the agreement or change your data storage location. In addition, some organisations may no longer wish to warrant that they will comply with EU law (including GDPR) if this is no longer applicable to them.

Update your compliance documentation: privacy notices, breach notification procedures, Data Protection Impact Assessments (DPIAs) or other documentation. Policies can already be updated to add a reference to "the EU and the UK" since, in any case, the UK will no longer be part of the EU. In addition, DPIAs may need to be updated to describe international transfers and describe the strategy for dealing with such transfers.

As a UK organisation, you should consider whether you should establish a branch office or affiliate in the EU, or transfer decisional powers to such establishment, in order to benefit from the one-stop-shop.

Make sure your appointed DPO in the UK for a group of undertakings is easily accessible from the EU.