The Law Society

No-deal Brexit: data protection

October 2018

Introduction

This paper forms part of a series published by the Law Society. The aim of this paper is to highlight the changes that will occur should the UK leave the EU on 29 March 2019 without having concluded an agreement with the EU beforehand.

In such a scenario, the EU and UK will have failed to sign both a Withdrawal Agreement (governing the terms of the UK's departure from the EU) as well as an agreement governing the future relationship between the two parties. Similarly, the transition period that has been provisionally agreed between the UK and EU will not apply.

This paper underlines the steps solicitors and firms should consider in order to prepare their practice for such an eventuality.

This note does not replace legal advice or a consultation on an individual basis with the relevant regulators/authorities. We cannot accept any liability resulting from any action or lack thereof taken on the basis of the information contained in this note.

Consequences of a no-deal Brexit

In its notice to stakeholders, the European Commission summarised the options for lawful transfers of EU personal data to the UK in the absence of an adequacy decision. Organisations may rely on safeguards set out in the GDPR. These include Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), certification and codes of conduct, and derogations (the latter applying to EU data exporters only).

In the event of a no-deal outcome, solicitors should focus on their data processes and the potential disruption to those that a no-deal outcome may cause. Solicitors should seek to mitigate such risks by implementing possible workarounds, while also bearing in mind their weak points. Solicitors will need to take appropriate actions to demonstrate their efforts to ensure compliance with the relevant data protection regime post-Brexit.

This can be done through:

- devoting proportionate and reasonable resources to identifying risk with their international data transfers

- mitigating that risk with the appropriate mechanism such as data subject consents, SCCs, BCRs, or certification and codes of conduct; and
- supporting this with the necessary governance, internal controls and staff training.

In following the above actions, solicitors will be well placed to be able to demonstrate best practice and compliance with GDPR and other relevant data protection laws in the face of the uncertainty caused by a no-deal outcome.

A more detailed description of each of the mechanisms mentioned above is set out below.

Points for solicitors to consider under a no-deal Brexit

Solicitors should generally be aware of the following points:

- Solicitors should review the data flows and transfer mechanisms in their firms to make sure there will be no breach in their data operations if there is a no-deal Brexit. This includes transfers of personal data from the EU to the UK and onward transfers of that data from the UK to third countries (in particular where contracts include clauses where transfer of data outside of the EU is prohibited).

- Solicitors should review which of the safeguards described below is best suited to the needs of their firm (i.e. SCCs, BCRs, etc.).

- If at present firms rely on the SCCs in transferring EU personal data outside the EEA to another controller or a processor outside the EEA, solicitors should consider putting in place a new mechanism for that transfer.

- Alternatively, solicitors may wish to consider changing their firms' data flows in relation to EU personal data so that it is transferred from an EU data exporter directly to a non-EEA/non-UK data importer under an appropriate data transfer mechanism (e.g. SCCs).

- In case a firm's processing relies on consent obtained while the UK is still a member of the EU, solicitors should consider obtaining it again, as it is unclear at the moment whether UK businesses relying on consent in processing EU personal data can continue to do so following a no-deal Brexit. This applies in cases where the consent had been obtained when the UK was still a member of the EU and does not specifically cover

transfer of personal data outside the EEA. Solicitors should closely examine the consent language to see if it specifically covers the transfer of personal data obtained outside the EEA.

- Solicitors should review their privacy policies so that clients understand the movements of their personal data in and outside of the EU.

- If you have an office in another EU country or process EU personal data, you should consider other aspects of local privacy laws in that country, as GDPR allows for local variations (e.g. in relation to data breach notifications, or appointment of a data protection officer, etc).

- If you have offices in other EU states and have nominated the ICO as your Lead Supervisory Authority (LSA) under the One Stop Shop principle, in a no-deal Brexit scenario the ICO will not be able to remain the LSA in relation to EU personal data, and you need to consider nominating another EU regulator as your LSA for the EU personal data, which should be chosen in accordance with the GDPR requirements. In case you do not have an office in another EU state, but will process EU personal data, you might have to appoint an EU representative and update your privacy notices to include their contact details.

You can find Standard Contractual Clauses (SCCs) here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. Please note that at the moment, the SCCs are being subject to the legal challenge in Ireland and referred to the Court of Justice of the EU (CJEU) (Case C-311/18). Since it will have an impact on the use of the SCCs in data transfers, you should monitor its outcome.

Current system

At present, the UK is party to many instruments which regulate processing of personal data, including transfers outside of the EU/EEA and the sharing of information.

These include the General Data Protection Regulation (**GDPR**) and the Law Enforcement Directive (**LED**). They also cover law enforcement information sharing systems, such as

Europol, the European Criminal Records Information System (ECRIS), Passenger Name Records (PNR) and the Europol Information System (EIS).

The GDPR, LED and information sharing systems facilitate the transfer of data between the UK and other EU member states. Both GDPR and LED set our legal bases for transferring personal data outside the EU/EEA. In the case of the GDPR, the relevant information is in Articles 44 to 49.

Post-Brexit, the UK will be considered as a 'third country' under EU rules. There are currently two possibilities for transferring personal data outside the EU/EEA to third countries: with or without an adequacy decision.

- Transfers with an adequacy decision do not require any additional safeguard or an authorisation (save for compliance with relevant laws and regulations).

- An adequacy decision is an implementing act adopted according to the examination procedure set out in Article 5 of the Regulation (EU) No 182/2011.

- This assessment is carried out by the Commission and informed by the EU's national data protection authorities, a model that is broadly maintained by the GDPR and LED. It is important to note that adequacy can apply to an entire country but also to specific sectors.

- The EU/US Privacy Shield allows data transfers to the United States which is a third country without an adequacy decision. It does so by conferring an adequacy decision on the mechanism of the privacy shield. This allows member organisations to process the personal data of EU/EEA data subjects.

- The safeguards for transfers without an adequacy decision include the Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), certification and codes of conduct, and derogations, such as explicit consent, fulfilling a contractual obligation, public interest, establishment, exercise or defence of legal claims or vital interests of the data subject.

No-deal scenario

Should the UK leave the EU under a no-deal scenario, it will become a designated third country. As a result, any transfers of personal data from the EU to the UK will need to fulfil the requirements of EU data protection law. Transfers from the UK to the EU, as indicated by the Government in its technical notice, will continue unchanged.[1]

However, it is unclear what rules will apply to onward transfers of personal data of EU citizens from the UK to third countries (i.e. non-EU/EEA).

It is possible that the UK will not benefit from an adequacy decision of the European Commission. The Commission is under no obligation to make this decision in favour of the UK. In any case, obtaining an adequacy decision may take a long time.[2] In the event of a no-deal scenario, therefore, there may be restrictions on the free flow of data between the EU and the UK.

Alternatives for businesses

In its notice to stakeholders, the European Commission summarised the options for lawful transfers of EU personal data to the UK in the absence of an adequacy decision.[3] Organisations may rely on safeguards set out in the GDPR. These include Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), certification and codes of conduct, and derogations (the latter applying to EU data exporters only).

1. Standard Contractual Clauses (SCCs)

The Commission adopted three sets of SCCs: two for EU/EEA controller to non-EU/EEA controller and one for EU/EEA controller to non-EU/EEA processor.[4] Many organisations already rely on the SCCs in their international business operations. However, SCCs cannot be employed in all circumstances. Moreover, they have not yet been updated to reflect the

[1] https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

[2] The process starts with a proposal from the Commission. To conclude its decision, the EU then needs the following: (a) an opinion of the European Data Protection Board, (b) approval from the representatives of all EU states and (c) official adoption of the decision by the Commission. It is important to note that the most recent adequacy decision (New Zealand) took the EU four years to adopt.

[3] https://ec.europa.eu/info/sites/info/files/file_import/data_protection_en.pdf

[4] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

GDPR and their validity is currently under review by the CJEU following a reference from the Irish High Court.[5]

SCCs can only apply between parties subject to the conclusion of a contract and cannot be used in certain instances, for example where there are joint controllers or a group of undertakings engaged in joint economic activity.

However, while that mechanism could allow UK-based organisations to continue to receive EU personal data, unless further measures are put in place by concerned UK organisations, whether acting as a data controller or a data processor, it will not be sufficient to allow them to transfer EU personal data (i.e. personal data to which the GDPR and member state privacy laws apply) onwards to a third country that does not have an EU adequacy decision. Many UK data controllers at present rely on the SCCs in transferring EU personal data outside the EEA to another controller or a processor. Following a no-deal Brexit, this mechanism, although sufficient for transfer outside the UK of UK personal data (in so far as UK law is concerned), will no longer apply to EU personal data. That is because, in the event of a no-deal Brexit, UK organisations will cease to be data exporters within the meaning of the GDPR and of other EU member states' privacy laws.

In cases where the UK organisation processes EU personal data as a data processor, this issue might be solved through the execution of the 2010 SCC with the EU-established data controller, and having a non-EEA based third-party, to which the UK organisation transfers EU personal data, to "join" the SCC as a sub-processor.

When the UK organisation acts as a data controller of EU personal data, under the 2004 controller-to-controller SCCs, it cannot transfer EU personal data onwards to a third-party controller established outside the EEA unless certain conditions are satisfied, one of which is that the third party must become a signatory to the SCCs.

However, this route is not possible when the UK organisation is a data controller and the third-party established outside the EEA is a data processor of EU personal data. Therefore, another mechanism (e.g. data subject consent) will need to be found to allow UK data controllers to transfer EU personal data to onwards to a non-EEA data processor.

[5] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems

2. **Binding Corporate Rules (BCRs)**

Another option for multinational businesses would be to adopt Binding Corporate Rules (BCRs), in accordance with Article 47 of the GDPR. These allow organisations to transfer personal data from the EEA within their group outside the EEA. Existing BCRs will remain good practice to demonstrate compliance with the GDPR. Although implementing a BCR takes a long time and requires substantial resources, if the process has already been launched, it would still be worthwhile to proceed with implementing BCRs even if the process is not complete by March 2019, as progress would serve to demonstrate compliance with best practice to the relevant regulator.

3. **Codes of Conduct and certification mechanisms**

Organisations in the UK may wish to consider adopting, through their trade association or representative body, approved Codes of Conduct or certification mechanisms together with enforceable and binding rules on the controller or processor. These instruments may also take time and substantial resources to adopt but if the process has already been started it would still be worthwhile to proceed with implementing a Code of Conduct, even if that process is not complete by March 2019, as progress would serve to demonstrate compliance with best practice to the relevant regulator.

Bilateral agreements with EU member states

As explained above, the EU has an established mechanism to allow the free flow of personal data to countries outside the EU, namely an adequacy decision. Member states do not have the competence to unilaterally grant adequate decisions to third countries. The UK would not be able to form bilateral agreements with member states on the cross-border transfer of data in areas governed by EU law, or in relation to databases governed by EU law.

Additional resources

Standard Contractual Clauses (SCCs): https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

UK Government Technical Notice: Data protection if there's no Brexit deal

European Commission Notice: Rules in the field of data protection