EVERSHEDS SUTHERLAND

Data protection and Brexit

What you can do to prepare

Uncertainty remains as to how data protection law will apply after the UK leaves the EU, depending on whether or not a deal is agreed.

After the historic defeat on 15 January of the draft withdrawal agreement (**defeated deal**), we consider below what the implications of a no-deal Brexit would be for data protection, and the extent to which the defeated deal would have dealt with any of those issues.

We also provide a checklist of actions that businesses can take to help prepare for the outcome in default – a "no deal" Brexit.

Background legal framework

Given the complexity of the issues raised by Brexit, we consider it helpful to set out some bare minimum details on the background law as it relates to data protection.

The European Union (Withdrawal) Act 2018 (**EUWA**) repeals the European Communities Act 1972 and empowers the government to legislate in order to deal with inadequacies in UK law arising from Brexit. It is also the instrument which will transpose the GDPR into the UK legal framework, so that the data privacy principles, obligations and rights that UK organisations and individuals have become familiar with will remain applicable post-Brexit. The EUWA is effective from **exit day,** which is defined as 29 March 2019 at 11 pm (N.B if the defeated deal had been agreed, this definition would have been amended via the European (Withdrawal Agreement) Bill to give effect to the defeated deal's transition period, i.e. until 31 December 2020).

The draft Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPECR) were laid before Parliament by the government on 19 December 2018 in exercise of its powers under the EUWA, to ensure that the UK data protection legal framework continues to operate smoothly after exit day. The majority of the DPPECR will come into force on exit day. However, certain provisions (Regulations 7 and 8 and Schedule 4) which align the definition of consent under Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) with the GDPR, and make consequential amendments under the Data Protection Act 2018 (DPA 2018) will definitely come into force on 29 March 2019.

The DPPECR create a single UK GDPR by merging and amending two pre-existing data processing regimes: (1) the GDPR as supplemented by Chapter 2 of Part 2 of the DPA 2018; and (2) the "applied GDPR" (Chapter 3 of Part 2 of the DPA 2018), which extended GDPR standards to processing activities outside of the GDPR's scope.

Defeated deal

If agreed, the defeated deal would have ensured that EU data protection laws (including GDPR and ePrivacy Directive) continued to apply in the UK until 31 December 2020 (i.e. the end of the transition period), and beyond if that was extended. The laws would have produced the same legal effects in the UK as they do for EU Member States. Therefore, transfers of personal data to the UK would not have been restricted until at least 31 December 2020. However, the ICO's participation in the EDPB and one-stop-shop would cease. After transition, the DPPECR would have applied in the UK.

In the accompanying political declaration on the future relationship between the UK and the EU (PD), published on 22 November, the EU committed to assess the UK against the EU's adequacy framework and to "endeavour" to make a decision in this regard before the end of 2020. A finding of adequacy would facilitate the seamless continuation of personal data transfers from the EU to the UK post-transition. The quid pro quo was that, in the meantime, the UK would take steps to facilitate transfers of personal data to the EU. In addition, the parties explicitly committed to make arrangements for the appropriate cooperation between regulators, which could have been interpreted as a nod to the potential continuation of the ICO's participation in the operation of GDPR's one-stop-shop mechanism in some form.

No deal

If no deal is agreed in advance of 29 March 2019, and Article 50 is not extended or revoked, the UK will become a "third country" after 29 March 2019 and will be treated as such. Therefore, the main issue as regards data protection is that transfers of personal data from the EU to the UK will be restricted.

Recently published guidance from the ICO and the UK Government's Department for Culture, Media and Sport (DCMS) on this scenario, makes the following points:

- the EUWA will retain the GDPR in UK law but the Government will make appropriate changes to the GDPR and the Data Protection Act 2018 to preserve EU GDPR standards in UK domestic law (see reference to the DPPECR above). Therefore, controllers' responsibilities will not change and the same GDPR standards will continue to apply in the UK.

- the extra-territorial scope of the UK data protection framework will be maintained in an equivalent manner as under the EU GDPR, so UK data protection laws will apply to overseas controllers or processors where they are processing personal data about individuals in the UK in relation to the offering of goods or services, or the monitoring of their behaviour. Note that this extra-territorial scope will apply to EU-based controllers and processors as well as those outside the EU. Equally, the extra-territorial provisions of the EU GDPR will apply to UK controllers and processors processing personal data about data subjects in the EU if they are not also established in the EEA.

- non-UK controllers who are subject to UK data protection law will be obliged to appoint representatives in the UK if they are processing data relating to UK data subjects, other than occasionally.

- the UK will transitionally recognise all EEA states, EU and EEA institutions and Gibraltar as providing an adequate level of protection for personal data, allowing free flow of personal data (although this decision will be kept under review). Existing EU adequacy decisions will be honoured on a transitional basis (these are currently in place for Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay).

- the UK cannot provide for free flow of data into the UK for businesses that rely on data transfers from the EU: those businesses will need to work with their EU. counterparts to make sure an alternative mechanism for transfer (such as standard contractual clauses) is in place.

- the Government intends to make arrangements for continued application of the US Privacy Shield framework for transfers from UK to US. Find further guidance from the United States Department of Commerce here, on additional steps required by organisations relying on US Privacy Shield for effective application post-Brexit.

- provision will be made so that the use of Standard Contractual Clauses (SCCs) previously issued by the European Commission will continue to be an effective basis for international data transfers to jurisdictions outside the UK and those recognised as adequate above. Where the existing EU SCCs have been used to safeguard transfers from the UK before exit day, they will continue to be valid (unless and until disapplied by the ICO or Secretary of State). The ICO and Secretary of State will also have the power to make provision for new SCCs for transfers outside the UK after exit day.

- existing authorizations of Binding Corporate Rules (BCRs) made under the EU process will continue to be recognised in UK law. After exit day the ICO will continue to be able to authorise new BCRs under UK law, but these would not automatically be recognised by other EU supervisory authorities.

Actions to take

In the event of a "no deal" scenario:

- Revisit your Article 30 data record and consider each of your data processing operations in isolation to identify any impacted activities.
- Assess the location(s) of your business establishments and the data subjects for each of your processing operations to help determine which data protection laws apply.
- Identify transfers of personal data to/from the UK and assess whether an "appropriate safeguard" is required under GDPR and whether any updates are required for your safeguard(s) to work effectively. Solutions available in the absence of a UK adequacy decision could be the SCCs, BCRs (for intra-group transfers), the EU-US Privacy Shield or reliance on a relevant derogation.
- Revisit contracts governing your data processing and sharing activities, and consider whether they need to be varied to continue to operate effectively.
- Consider whether you need to appoint an EU-based or UK-based representative under GDPR or UK data protection laws.
- If your main establishment is in the UK, note that you will no longer benefit from the one-stop-shop. However, note that you may (depending on the structure of your organisation) be able to identify an alternative main establishment within the EU and therefore benefit from the one-stop-shop in respect of your non-UK processing. You can find the EDPB guidance on this topic here.
- Consider the requirements to appoint a data protection officer (DPO) under GDPR and UK law, and assess whether your DPO is "easily accessible" from each establishment in the UK and EEA, as applicable.
- Revisit data protection impact assessments relating to processing activities involving international data transfers which may become restricted post-Brexit.
- Review and amend your data protection compliance documentation, such as your data records, policies and privacy notices to accurately document transfers of personal data to/from the UK and the contact details for your EU-based and/or UK-based representative(s) and data protection officer(s), as applicable.
- Keep an eye out for further guidance on the ICO's involvement in the one-stop-shop and EDPB, and territorial scope and data transfers. (N.B. At the time of writing, it is unclear under draft EDPB guidance how EEA-based processors are expected to comply with GDPR rules around transfers. See our briefing on this topic here.)

For more information about the data protection implications of Brexit please contact:

Paula Barrett
Co-Lead of Global Privacy and Cybersecurity

T: +44 20 7919 4634
M: +44 777 575 7958
paulabarrett@eversheds-sutherland.com

Gayle McFarlane
Partner

T: +44 20 7919 1262
M: +44 739 325 4408
gaylemcfarlane@eversheds-sutherland.com

Liz Fitzsimons
Partner

T: +44 122 344 3808
M: +44 774 091 8238
lizfitzsimons@eversheds-sutherland.com

eversheds-sutherland.com

LON_LIB1\19851604\2