HM Government

UK LEAVES THE EU 29.03.19

Data Protection if there is no EU Exit deal

1. Overview

- Leaving the EU with a deal remains the Government's top priority; this has not changed.
- The Government has accelerated **'no deal'** preparations to ensure the country is prepared for every eventuality – it is the responsible thing to.
- In the event that the UK leaves the EU on 29 March 2019 without a deal, UK businesses will need to ensure they continue to be compliant with data protection law.
- The General Data Protection Regulation (GDPR) will be brought into UK law, meaning that current GDPR standards and existing guidance will continue to apply to businesses operating within the UK.
- The GDPR contains additional rules to protect data that is transferred outside the EEA (known as restricted transfers). From 29 March 2019, if there is **'no deal'**, these rules will apply to data transferred from the EEA to the UK.
- The rules on transferring data to a non-EEA state are simpler if the European Commission has decided that data is adequately protected in that state. If the UK exits without a deal on 29 March 2019, we do not expect the European Commission to issue an adequacy decision in time. This means that UK businesses must act now to comply with the GDPR rules on international transfers if they are transferring personal data across borders.
- The UK does not intend to impose additional requirements on transfers of personal data from the UK to the EEA, therefore, businesses will be able to send data to the EEA as they do currently. However, businesses will need to update their documentation and privacy notices as appropriate.

Case Study: personal data transfer from EEA to UK

An Italian travel agent sells holidays in the UK. In order to fulfil the bookings, it sends the personal data of customers (names, dates of birth, postal address) to hotels in the UK. The UK hotels require this data to operate. After the UK leaves the EU this will become a restricted transfer and the UK hotels will need to work with the Italian travel agent to ensure action is taken to keep the data flowing.

2. What do businesses need to do to prepare?

- As a priority, UK businesses need to review their international data flows to identify any personal data they receive from the EEA. *For example an international transfer of personal data could be: where UK companies use centralised or outsourced HR services in the EEA to process employee and payroll details; or receiving customer information from the EEA, such as names and addresses, in order to provide goods or services.*
- UK businesses, with their EEA partners, need to consider what GDPR safeguards they can put in place to ensure that personal data can continue to flow **from** the EEA **to** the UK once we have left the EU.
- The GDPR sets out a range of different options that allow organisations to make restricted transfers, including appropriate safeguards. Further information can be found in the links below.
  - One appropriate safeguard that can be used by many businesses are standard contractual clauses (SCCs). These are pre-approved by the European Commission and can be inserted into contracts to provide a legal basis for transferring personal data from the EEA to the UK. The ICO has produced an interactive tool to help businesses understand and complete SCCs for their personal data transfers from European partners: **http://bit.ly/ico-tool**
  - Businesses that are part of a multinational group may be able to rely on binding corporate rules (BCRs), for intra-group transfers as an appropriate safeguard.
  - In specific situations transfers are permitted without additional safeguards where one of the exceptions apply as found under Article 49 of the GDPR.

3. What resources are available?

Information Commissioner's Office	Guidance and resources to prepare for EU-exit Leaving the EU – six steps to take Detailed guidance on data protection if there is **'no deal'**
HM GOV information on 'No Deal' EU Exit	Information on 'No-Deal' EU Exit and data protection

The government, and the Information Commissioner, will continue to provide guidance and information to businesses and other organisations to help them understand how they will need to operate under a range of outcomes on data protection, and plan appropriately.