DATA PROTECTION AND ‘NO DEAL’ BREXIT

The possibility of the United Kingdom (UK) leaving the European Union (EU) without a deal, even at the end of any extended period agreed with the EU, is a real risk for businesses to consider and plan for. This note explains key issues and steps to be taken to plan in relation to personal data protection in the event of a ‘no deal’ Brexit.

WHAT HAPPENS ON ‘NO DEAL’?
Under such a ‘no deal’ scenario, the EU’s General Data Protection Regulation (GDPR), will form part of UK domestic law by virtue of the EU (Withdrawal) Act 2018 (EUWA) with some amendments made to it, alongside the UK’s Data Protection Act 2018 (DPA) and the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (Exit Regulations), which will come into force on exit day, replace references to EU laws and institutions with references to UK equivalents, so that the UK’s legal framework for data protection can function correctly after exit day. The Exit Regulations also provide that the UK GDPR will have extra territorial effect in the same way as the EU GDPR. This means that the UK GDPR will apply to controllers and processors outside the UK whose processing activities relate to offering goods or services to individuals in the UK or to the monitoring of the behaviour of individuals in the UK.

BUSINESS AS USUAL AS FAR AS POSSIBLE?
There would be no immediate change in the UK’s data protection standard because the DPA will continue to apply and the provision of the GDPR will be incorporated directly into UK law. The UK government also confirmed that transfers of personal data from the UK to the EEA will not be restricted.

From a UK perspective, no immediate steps need to be taken if an organisation has appointed a data protection officer (DPO), who is either based in the UK or EEA, provided that such DPO is easily accessible to all and is sufficiently skilled in both EU and UK data protection laws. However, this should be kept under review.

WHAT NEEDS TO BE ADDRESSED?
The key points to consider in case of a ‘no deal’ Brexit from a data protection perspective are:

- EU to UK personal data transfers
  The UK becomes a third country, which means in the absence of adequacy decisions for the UK, new safeguards will need to be considered for the transfer of personal data from the EU to the UK as well as onward transfers of that data from the UK to third countries.

- Choosing an alternative lead supervisory authority (LSA) from the UK
  Organisations will no longer be able to appoint the UK’s regulator (the Information Commissioners’ Office (ICO)) as their lead supervisory authority for EU GDPR compliance and will need to consider appointing a new lead supervisory authority from an EU member state.

- Appointment of EU representative
  Organisations who are bound by the EU GDPR who are required to appoint a representative in the EU will not be able to rely on a UK representative and may need to appoint a different EU representative.

- Appointment of UK representative
  Organisations who are based outside the UK but bound by UK data protection laws by virtue of their extra-territorial impact (including organisations in the EU) will need to consider appointing a UK representative.
Updating records on international data flows

Controllers and processors that are obliged to keep records under Article 30 of the EU GDPR on transfers to ‘third countries’ will now need to update their records to identify transfers from EU to the UK and the compliance mechanism being used for such transfers. UK controllers and processors should also record transfers from the UK to the European Economic Area (EEA).

HOW TO CONTINUE TRANSFERRING PERSONAL DATA TO THE UK

As mentioned above, once the UK has left the EU, it becomes a third country from an EU perspective. This means the GDPR requirements for transferring data to third countries will apply, ie personal data that is transferred to the UK from the EU must be have adequate levels of protection, for example:

- an adequacy decision is made by the European Commission confirming that the UK has adequate protections in place to safeguard personal data;
- binding corporate rules (BCRs) are entered into to ensure personal data can easily be transferred between group companies; or
- standard contractual clauses (SCCs) adopted by the European Commission.

The UK government is planning on seeking an adequacy decision from the European Commission for the UK. This means that the UK’s data protection regime would be recognised by the European Commission as ‘essentially equivalent’ to those in the EU. As a result, data will be able to flow from the EEA without the need for organisations to adopt any other specific measures to allow the international transfer of personal data. This arrangement will not be in force immediately post-Brexit as the European Commission’s assessment as to whether the UK’s data protection regime is ‘essentially equivalent’ will only start when the UK has left the EU, ie when the UK is a third country.

In the absence of an adequacy decision regarding the UK at the point of the UK leaving the EU, UK organisations that want to receive personal data from organisations established in the EU should work with their EU partners in identifying a legal basis for those transfers such as the BCRs and SCCs, as mentioned above.

For most organisation the most relevant alternative legal basis would likely be the SCCs. The SCCs are still in their pre-GDPR form as they have not yet been updated. While this mechanism would allow UK based organisations to continue to receive personal data from the EU it will not be sufficient (without further measures being put in place) to allow UK organisation to transfer EU personal data to a third country that does not have an EU adequacy decision. Whereas, transfers of personal data from countries outside the EU to the UK are likely to remain the same.

Depending on the size of the organisation, the organisation may decide that putting BCRs in place will ensure that personal data can easily be transferred within the organisation. To date, only a limited number of international organisations have put BCRs in place as they are very time consuming to put in place, however, going forward this may change. Organisations who use approved BCRs or have applied for BCRs with the ICO for their approval of their BCRs will need to identify a new EU/EEA supervisory body as their LSA. Any existing BCRs also need to be updated to list the UK as a third country.

A transfer from the UK to the EU/EEA (for example to an EU group company acting as a controller or a processor), where the personal data is then transferred back to the original data exporter in the UK in theory does need to be considered as a transfer of data from the EU/EEA entity to the UK entity. Where the EU entity is a processor and the UK entity is a controller, there are no specific ‘processor-to-controller’ clauses which neatly cover this scenario, so further guidance from the European Data Protection Board (EDPB) would be welcomed on this point.

HOW TO CONTINUE TRANSFERRING PERSONAL DATA FROM THE UK

As mentioned above, transfers of personal data from the UK to the EEA will not be restricted. Furthermore, the Information Commissioner is preserving the availability of the Privacy Shield for UK personal data flows to the US. However, to take advantage of this, Privacy Shield-certified companies will need to expressly state in their Privacy Shield Policies their commitment to applying the Privacy Shield Principles to UK personal data. They will also need to make this commitment clear in their Human Resources (HR) privacy policies if importing HR data from the UK.
In addition, transfers of personal data from the UK to countries outside the EEA are likely to remain similar to the pre-Brexit position. This is because the UK government has confirmed there will be transitional arrangements to recognise:

- most existing EU adequacy decisions;
- the SCCs; and
- the BCRs.

As mentioned above, if an organisation is relying on BCRs, they will need to be updated to reflect that the UK is a third country and if such BCRs have been authorised by the ICO, they will need a new LSA within the EU/EEA.

ESTABLISHING WHO THE NEW LEAD SUPERVISORY AUTHORITY IS

Under the GDPR, the LSA coordinates cross border processing across the EEA. This is important for organisations that have establishments in more than one EEA member state, but also for organisations who deal with data subjects based in more than one EEA member state. The LSA is responsible for conducting investigations into the organisation’s data processing activities and respond to its compliance enquiries. After the UK has left the EU, the ICO will no longer qualify as a LSA under the GDPR, which means organisations will have to deal with both the ICO and the relevant EU LSA. The ICO will collaborate with European supervisory authorities regarding any breaches of GDPR that affect individuals in the UK and other EU and EEA member states. The ICO recommend that UK organisations should consider:

- whether their processing of personal data involves cross-border processing under the GDPR;
- whether to carry out cross-border processing after exit date;
- which other EU and EEA supervisory authority will become lead authority on exit date (if any). You may want to consider the EDPB guidelines for identifying a controller or processor’s lead supervisory, which you can find [here](#).

APPOINTING A REPRESENTATIVE IN THE EU

Under article 27 of the GDPR, organisations (irrespective of whether they are data controllers or data processors) who are not established in the EU, but are either:

- offering goods or services to data subjects based within the EU; or
- monitoring the behaviour of data subjects based within the EU,

will be required to appoint a representative within the EU. The purpose of this obligation is ensuring that supervisory authorities and data subjects have a point of contact within the EU. It is important that the representative is appointed in one of the EU member states where the data subjects that are affected by the processing are located, however, it is not necessary to appoint one for each member state.

The following should be taken into account when appointing a representative:

- the appointment must be in writing;
- no specific obligations or requirements in respect of the representative’s qualifications or its connection with the organisation. This means a third party representative can be appointed; and
- the representative must have authority to act on behalf of the organisation, however, this does not affect the liability of the organisation appointing the representative.

Post-Brexit organisations that do not have a presence in the EU or the UK, but intend to offer goods and services and/or monitor individuals located in the UK and the EU/EEA may require both a UK representative under the UK GDPR and an EU/EEA representative under EU GDPR. For example a company in the US, which has no EU offices, presently needs an EU representative if it is intending to sell goods to individuals located in the EU. After Brexit, this US company would need both an EU and a UK representative if it wishes to continue to sell goods to individuals in the EU and the UK. This is because the company only has a presence in the US, but intends to sell goods to individuals in both the EU and UK.
CONCLUSION

Therefore, under a ‘no deal’ Brexit, organisations should, among other things:

- review their data flows and transfer mechanisms to make sure there will not be in breach of their data operations, but also ensuring that their business partners in the EU can continue to share personal data with them;
- consider which safeguards are best suited to their needs (for example, SCCs, BCRs, etc);
- update records regarding international data transfers to include UK/EU data transfers;
- establish which EU supervisory authority will become the new LSA in respect of cross border transfers within the EU; and
- consider appointing an EU representative and/or UK representative and updating privacy notices to ensure that they are transparent about the organisation’s processing.

FIND OUT MORE

For further information, please contact:

**JOANNE VENGADEN**
T: +44 (0)118 402 3833
E: joanne.vengadesan@penningtons.co.uk

**NORA POOK**
T: +44 (0)1865 813737
E: nora.pook@penningtons.co.uk

Please note: Specialist advice should be obtained before taking, or refraining from taking, actions based on comments in this update which is only intended as a brief note. © Penningtons Manches LLP, 2019.