BREXIT DATA PROTECTION TIPS

The Brexit transition clock is ticking. At 11pm UK time on the 31st of December 2020, all UK organisations that transfer data to or from the EU will need to have taken appropriate steps to prepare for the post-Brexit landscape. Here are our 11 Brexit data protection tips that will help you to plan and prepare for the arrival of the UK GDPR.

1 MAP YOUR DATAFLOWS - UNDERSTAND ANY INTERNATIONAL TRANSFERS

The first step in your data protection Brexit planning should be to gain a thorough understanding of your data flows. You need to understand if personal data is being transferred out of the UK, accessed or processed by EU Processors/Controllers or if you are importing personal data from the EU or offering services/ monitoring the behaviour of EU residents. Understanding your dataflows will assist with determining if the current transfers can continue post Brexit or if additional safeguards will be need to be implemented.

2 PREPARE FOR NO ADEQUACY - IMPLEMENT TRANSFER SAFEGUARDS

In the absence of an adequacy agreement with the EU, additional safeguards must be implemented to continue lawfully transferring personal data from the EU to the UK. Based on the outcome of your data mapping exercise, if an appropriate transfer safeguard, such as Standard Contractual Clauses (SCCs), is not in place, incorporate these into each of the contractual agreements you have with your third party data providers/recipients, prior to 31st Dec 2020.

3 THE ONE STOP SHOP IS COMING TO AN END IN THE UK. NOMINATE YOUR NEW LEAD AUTHORITY

As it is currently understood, after Exit Day, the UK ICO will no longer participate in the one stop shop mechanism. If you have nominated the UK ICO as your lead authority under the One Stop Shop then this needs to be reviewed. If applicable, identify one of your alternative establishments situated within the EU and nominate that member state's authority as your new lead authority. This establishment must however, be responsible for making processing decisions, otherwise they may not qualify and therefore you will no longer be able to take advantage of the One Stop Shop. Where a change is made, remember to update your policies to reflect that change.

4 CONFIRM IF YOU NEED TO APPOINT AN EU OR UK REPRESENTATIVE

Do you provide goods or services to the EU? Do you monitor the behaviour of EU Residents? If you do, and you don't have a suitable establishment/ office in the EU then you may need to appoint an EU Representative as required by EU GDPR Article 27. The same applies in reverse if you are an EU organisation under UK GDPR.

Head Office
The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

Registered Office
Suffolk Enterprise Centre
Felaw Street
Ipswich IP2 8SJ

Dublin Office
Alexandra House
3 Ballsbridge Park
Dublin D04 C7H2 Ireland

Contact Us
0203 797 1289
hello@dpocentre.com
www.dpocentre.com

Outsourced Data Protection

BREXIT DATA PROTECTION TIPS

5 PREPARE AMENDMENTS TO BREACH PROCEDURES AND NOTIFICATION PROTOCOLS

If you have offices in other EU member states and especially if you are utilising the 'One Stop Shop' mechanism, it is likely that your breach procedures and notification protocols will need to be amended to reflect these changes. Identify which supervisory authority you will need to notify (or which is applicable in various circumstances if the OSS is no longer available to you) and how you will ensure the correct reporting measures are made within the permitted time frame from each relevant jurisdiction.

6 ENSURE PRIVACY SHIELD ORGANISATIONS HAVE UPDATED THEIR PRIVACY POLICY*

The UK has confirmed that it will recognise the EU/US Privacy Shield mechanism, however in order for it to apply to UK/US transfers, the US organisation must make a reasonably simple update to their public facing privacy policy to include the model language for UK transfers under privacy shield. Confirm that all your appropriate US partners have made this change.

*Since posting this tip, the Privacy Shield has been invalidated by the Schrems II decision by the CJEU, therefore this transfer mechanism can no longer be relied upon.

7 IMMEDIATELY AFTER EXIT DAY UPDATE YOUR PRIVACY POLICY

Regardless of whether the outcome of the adequacy decision is positive or negative, or if there is no decision at all, the UK will still become a 3rd country for the purposes of the EU GDPR from the 1st of January 2021. Therefore ensure you have updated the wording in your privacy policy to reflect this.

8 UPDATE YOUR POLICIES TO REFLECT WHICH LAWS WILL APPLY AFTER EXIT DAY

The UK will incorporate the GDPR into our legal system as the "UK GDPR" at the end of the transition period (31st of December 2020). The Data Protection Act 2018 will continue to apply in the UK as it does now, but will reference the UK rather than EU GDPR. Depending on whether you will be processing EU resident data, UK resident data or both, it is important to update your policies to state which law will apply to each data subject group, as the different legislation types are likely to diverge over time.

9 REVIEW ALL CONTRACTS TO ENSURE THEY REFER TO UK RATHER THAN EU DATA PROTECTION LAWS

From the 1st of January 2021 the UK will no longer be directly subject to EU data protection laws. From that date, we will be subject to UK data protection laws and therefore all your contracts and agreements (such as your general terms of business) that give reference to EU laws will need to be updated to UK laws as applicable.

10 WHERE RELEVANT, CONDUCT DPIAs AND UPDATE YOUR RoPA

Data Protection Impact Assessments (DPIAs) are a mechanism that enable you to identify the data protection risks associated with specific processing activities, including cross boarder personal data transfers, especially where those activities involve 'sensitive' personal data. Along with other details, your Records of Processing Activities (RoPA) then enables you to articulate this information. Therefore, if any of your processing will be changing as a result of Brexit, updates will be required.

11 IF RELYING ON SCCs, ENSURE YOUR VENDORS' NATIONAL LAWS DO NOT VIOLATE THE PROTECTIONS AFFORDED TO THEM UNDER GDPR

If you are relying on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), you are required to conduct a case-by-case analysis of each of your transfers to assess if 'adequate protection' is being provided within the legal framework of the receiver's country or jurisdiction. If these national laws violate these protections, the transfer is unlikely to comply with the GDPR so can no longer be used as a safeguard for transfers of personal data to that country.

Head Office
The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

Registered Office
Suffolk Enterprise Centre
Felaw Street
Ipswich IP2 8SJ

Dublin Office
Alexandra House
3 Ballsbridge Park
Dublin D04 C7H2 Ireland

Contact Us
0203 797 1289
hello@dpocentre.com
www.dpocentre.com