Roxburgh Milkins

Brexit Countdown - Data Protection Compliance

December 2020

For more information call +44 (0)117 928 1910 or visit www.roxburghmilkins.com

Roxburgh Milkins Limited, Merchants House North, Wapping Road, Bristol BS1 4RW

Introduction

We are fast approaching the end of 2020 and, with it, the end of the Brexit transitional period. The Government has consistently maintained that - deal or no deal - the UK will no longer be a member of the European Union (**EU**) on 1st January 2021.

Whilst the UK and EU continue to work hard towards reaching agreement on a post-Brexit deal, businesses are being urged to prepare for a no-deal scenario. The UK Gov website has a dedicated section dealing with the impact of Brexit on trading rules - https://www.gov.uk/transition.

In this guidance note, we look at the effect Brexit will have on data protection compliance, particularly for those businesses which send and receive personal data cross-border, to and from the European Economic Area (**EEA**), if there is no deal regarding data protection.

UK laws to remain the same

The Government has confirmed that the UK will remain fully aligned with the EU's data protection law - the General Data Protection Regulation (GDPR) - following Brexit, and the EU (Withdrawal) Act 2018 brings the GDPR into UK law after exiting the European Union.

This means that the laws and requirements relating to the collection, storage, use and processing of personal data will remain the same for data controllers and data processors within the UK.

The UK will also recognise the countries in the EEA, and Gibraltar, as having an 'adequate' level of protection, meaning UK businesses can continue to transfer data to those countries after Brexit, without the need for additional measures.

Operating/selling in the EEA - data protection implications

If you operate in the EEA, and have offices/branches in any part of the EEA, the GDPR is likely to continue to apply directly to those operations. If you transfer personal data from those offices/branches outside of the EEA (including to a branch/group company in the UK), you will need to comply with the GDPR rules relating to international transfers (see below for further information).

If you don't have any business operations in the EEA **but** you target any of your goods and/or services to EEA residents, or monitor the behaviour of EEA residents, the GDPR may still apply to you directly. In this case, you will be required to appoint a representative in the EEA (in a member state where some of the individuals whose personal data you process are located).

This representative must be authorised, in writing, to act on your behalf regarding your EU GDPR compliance, and to deal with any supervisory authorities or data subjects for you. This could be an individual with the requisite expertise but, more commonly, a professional services firm would be used.

The rules around the territorial scope of the GDPR - and whether it applies directly to your business - can be complex and depend on the nature of the business operations. If you'd like more information on this topic, please contact us.

International transfers - warning for importers of personal data from the EEA

As it stands - and without a deal - the UK will not be deemed an 'adequate' country for the transfer of personal data from the EEA. This means that businesses in the UK cannot be assured of the seamless flow of personal data from the EEA countries. Businesses that rely on data transfers from the EEA to the UK will need to put alternative mechanisms in place to continue such data transfers.

If your business receives personal data from controllers in the EEA, or data which pertains to EU citizens, you should be prepared to agree alternative data transfer mechanisms with those transferring the data to you. The most typical method used is the inclusion of standard contractual clauses, based on the EU model contract clauses, which will require you and the transferor of the data to enter into a contract variation or new agreement.

Unusually, even using a data processor in the EU as a UK business will mean that your processor will be subject to the GDPR transfer requirements and must have an appropriate mechanism in place in order to transfer personal data back to the UK. There are currently no standard contractual clauses in force for this scenario, though the EU is consulting on a new set of standard contractual clauses which includes processor to controller transfers. It is expected that these will be finalised in the New Year.

Practical steps to take

Here are a few key practical steps you can take to assess your data protection compliance and make any necessary changes:

1. Audit your data processing

The best starting point is to assess which personal data you process, where it originates from, and where it goes. In particular, consider:

1) Are you processing the personal data of EEA data subjects as a data controller?

2) Are you processing the personal data of EEA data subjects as a data processor for a third party?

3) If yes in either case, are you doing that exclusively via local EEA branches/offices or does the data leave the EEA for processing?

4) Do you transfer the personal data to any other controllers or processors? If so, where are they based?

Your findings will help you to determine the amount of work required to address and comply with the new cross-border transfer rules.

2. Consult ICO guidance

The Information Commissioner's Office, as the UK's supervisory authority for data protection, is regularly issuing guidance for businesses on the effect of Brexit.

You can find the ICO's resources online at https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/, including guidance for both SMEs and larger organisations.

In particular, the ICO website has a useful interactive tool to help businesses decide what they need to do in order to keep EEA data flowing post-Brexit - https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/.

3. Cross-border compliance

If you do have local EEA branches/offices, they should already be aligned with the GDPR requirements, but will now need to justify any transfer of personal data to the UK-arm of the business.

If their data flows can be segregated, so there is no cross-border transfer, it may simplify the compliance demands on the business.

If that is not possible, there would need to be an appropriate mechanism for the transfer of the personal data, which could include either binding corporate rules or a data transfer agreement containing the standard contractual clauses.

4. Finding an EEA representative

If you target your goods and/or services at EEA residents and routinely market and sell to EEA residents, or otherwise monitor EEA residents, you may be required to comply directly with the GDPR and appoint an EEA representative.

5. Incorporating the standard contractual clauses

As stated above, the EU's standard contractual clauses are one of the most common mechanisms used for transferring personal data outside of the EEA. These clauses, issued by the European Commission, will continue to be effective under UK law. These are meant to be used for international data transfers, where no adequacy decision has been made and no other basis for the transfer exists.

If you receive personal data from the EEA, and don't already have standard contractual clauses in place, you may need to update your contracts to incorporate them.

As the standard contractual clauses are currently under consultation for review, you should also consider including an obligation on the parties to enter into the new contractual clauses once they are issued.

Conclusion

The good news is that, for many businesses processing personal data in the UK, it will be business-as-usual as the laws will remain the same. The situation is more complicated for businesses which import personal data from the EEA, or those which have operations within the EEA. However, there are valid mechanisms in place for such businesses to continue transferring and using personal data. It is simply a case of reviewing how you send or receive personal data across borders and implementing the most appropriate mechanism(s) for your business and data flows.

Of course, we all hope that a deal will be reached before the end of the year. However, it is important to start planning for a no-deal scenario now, so you can maintain your compliance and keep the data flowing come 2021.

Contact us

This note is provided for general guidance only and should not be relied upon as legal advice. If you'd like advice or information regarding your data protection compliance, please do not hesitate to contact us at commercial@roxburghmilkins.com.