SQUIRE PATTON BOGGS

Brexit Transition Planning

Data Privacy Compliance

The UK withdrew from the EU on 31 January 2020.

The parties are now rapidly approaching the end of a transition period that was aimed at giving the EU and the UK time to agree on aspects of their future relations, including personal data flows between them. At the time of writing, the position remains unclear, which means that:

- Unless the UK obtains an adequacy decision from the European Commission (or some other form of agreement is made) before 31 December 2020, appropriate safeguards in accordance with the GDPR will need to be put in place to lawfully transfer personal data from the EU/European Economic Area (EEA) to the UK (unless one of the narrow derogations applies)
- It is possible that the same issues will arise in the reverse direction in regard to transfers of UK personal data to the EU/EEA pursuant to the UK Data Protection Act 2018

With less than two months to go until the end of the Brexit transition period, companies should now begin to plan for the worst-case scenario by taking the steps necessary to be in a position to react quickly if EU/EEA-UK data flows suddenly become unlawful, absent action on the part of data exporters and data importers.

Given the current uncertainty, businesses should be planning now. Identifying affected intra-group, customer and vendor arrangements and preparing priority action plans are crucial first steps. To help clients navigate this process, we have prepared a checklist of due diligence questions to be addressed and actions to be considered in the table below. Following the checklist, we have also provided a list of "known unknowns" that could impact the outcome of the Brexit transition negotiations in regard to transfers of personal data.

Please contact any of our GDPR experts listed at the end of this document or your usual point of contact at the firm if you have any questions or require support in preparing for the realities of conducting business post-Brexit transition in 2021.

Personal Data Flows: Organisations Are Advised to Review and Map Their International Data Flows	
Due Diligence Questions	**Actions to Prepare For**
• Identify personal data flows. Where is data being transferred from and to? From the EU/EEA to the UK? • From the UK to the EU/EEA? • Are these intra-group data flows or with external parties, such as customers and service providers? • Identify any data flows (contracts, internal flows, etc.) involving business-critical data, large volumes of personal data, special categories of personal data or personal data relating to criminal offences and records. • Identify GDPR Data Transfer Agreements (Standard Contractual Clauses) that cover combined EU/EEA and UK transfers to third countries outside the EU/EEA (e.g., the US) in order to assess if the agreements are Brexit-proof or require amendment to address UK to third-country transfers.	• Devise a plan to ensure that personal data flows between the EU/EEA and the UK (prioritising critical, sensitive or high volume data transfers) can continue lawfully on 1 January 2021. • Regularly check European Commission adequacy decisions and supervisory authority guidance on data transfers from the EU/EEA to the UK, or consult with us. • Be ready to enter into Standard Contractual Clauses to govern both intra-group and external data transfers from the EU/EEA to the UK (and potentially vice versa) in the event the UK does not obtain an adequacy decision or other agreement by 31 December 2020.
• Does your organisation rely on Binding Corporate Rules (BCRs) for transfers? Which supervisory authority were they approved by?	• If the BCRs were previously approved by the Information Commissioner's Office (ICO), seek to get them approved by a new EEA supervisory authority (in the EEA country where your organisation has its main EEA establishment) prior to 31 December 2020. • If your organisation has BCRs, prepare to update these to reflect the agreed methods of transfer of personal data to the UK, as necessary.

Consider Your Lead Authority Due to the Potential Change in the ICO's Role as a Supervisory Authority	
Due Diligence Questions	**Actions to Prepare For**
• If you are a multinational organisation with cross-border processing in the EU/EEA and the UK, is the ICO your lead authority at present? • Where do you have other offices in the EEA? If so, can one of them be considered a place of central administration or can it be turned into a place of central administration? • Have you checked if there are local forms or procedures to follow for notification of a new lead supervisory authority?	• If your lead authority is the ICO, consider if any other locations in the EU/EEA could fall under the definition of "main establishment" for a potential change of the lead authority and send the necessary forms to the new lead authority before 31 December 2020.

Consider Appointing a Representative in the EU/EEA (Article 27 GDPR), if You Do Not Have Presence in the EU/EEA	
Due Diligence Questions	**Actions to Prepare For**
• Does your organisation offer goods or services to individuals in the EU/EEA or monitor their behaviour in the EU/EEA, but has no establishment in the EU/EEA? • Might an exemption for an appointment of an EU/EEA representative apply to you? Check by answering the following question: Is your processing of individuals' data (a) occasional, does not include processing of special categories of data on a large scale or processing of personal data relating to criminal records, and (b) unlikely to result in a risk to the rights and freedoms of individuals?	• If you intend to continue to offer goods or services to individuals in the EU/EEA or monitor their behaviour in the EU/EEA post 31 December 2020 but have no presence in the EEA, then unless you fall within the narrow exemption, your organisation may need to appoint a representative in the EU/EEA. • Consider options available for appointing an EU/EEA representative for compliance with the requirements of the GDPR.

House-keeping Action Points

Once the position on the data protection rules for data transfers between the UK and the EU/EEA become clearer, the following tasks may be addressed:

- Amend privacy notices and records of processing to reflect the fact that the UK is a third country, if that is the case. Explain the safeguards that have been put in place for such transfers and identify any representative appointed.
- Amend data protection sections of contracts between the group companies and with external third parties by adding the agreed adequacy safeguards and updating EU/EEA references to reflect the fact that the UK is no longer part of the EU/EEA. If necessary, consider security measures to adopt for transfers to the UK in line with the Schrems II[1] ruling (e.g. encryption, any supplementary measures required by EU/EEA supervisory authorities), if the agreed appropriate safeguards are the Standard Contractual Clauses.
- Review Data Protection Impact Assessments to reflect the appropriate safeguards that are put in place for transfers to the UK.

1 On 16 July 2020, the "Schrems II" judgment of the Court of Justice of the EU (CJEU) invalidated the EU-US Privacy Shield regime and reiterated the importance of making a prior assessment of the ability of the data recipient in a third country to comply with their commitments under the Standard Contractual Clauses (SCCs). Post-Schrems II, organisations must carry out a prior regulatory risk assessment in relation to SCCs and BCRs to evaluate whether EU data subjects' rights will be protected and subject to due process when their personal data is transferred to a third country. From 1 January 2021, this judgment will likely apply to transfers of personal data from the EU/EEA to the UK in the absence of an adequacy finding or an extended transition period.

Overview of the Key "Known Unknowns" at This Stage

UK

The current position is that very little will change under the UK GDPR as compared to the EU GDPR. The UK government has indicated that it intends:

1. To continue to recognise that the EU/EEA ensures an adequate level of protection for personal data, so that personal data transfers from the UK to the EEA can continue without additional measures
2. To continue to recognise the European Commission's adequacy decisions so that the flows of personal data to those countries deemed to provide adequate level of data protection can continue for the moment without additional measures
3. To continue to recognise BCRs approved by the ICO for the purposes of data transfers outside the EU/EEA

However, this position could change, depending on the results of the negotiations between the UK and the EU and the impact on overall trade and diplomatic relations between the EU and the UK. For example, it is unclear whether the UK will opt to apply "non-adequate" status to the EU if the EU takes steps that could adversely impact data flows from the EU/EEA to the UK.

EU/EEA

The European Commission is in the process of negotiating new post-Brexit trade relations with the UK, but the ultimate model for the relationship going forward remains an open issue. It remains to be seen whether, in light of the Schrems II judgment and another recent decision of the EU Court of Justice finding[2] that aspects of the UK Investigatory Powers Act infringe EU law, the European Commission will be able to justify a positive adequacy assessment in regard to the UK even if there is an amicable conclusion to the Brexit transition and trade negotiations.

US

It is possible that separate trade negotiations between the US and the UK could result in a UK adequacy finding *vis-a-vis* the US when the UK is no longer subject to the jurisdiction of the EU Court of Justice. This could open up data flows between the UK and the US, but could also harden the position of the EU against the UK and lead to the EU to treat the UK the same as the US for data transfer purposes.

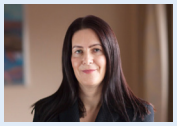
If you have any questions or require assistance with the due diligence efforts, do not hesitate to contact the team members listed here or your customary firm contact.Updates on this topic will be available on our Blog, Security & Privacy//Bytes. You may subscribe here.

Contact Us

Rosa Barcelo
Co-Chair, Data Protection & Cybersecurity practice, Brussels
T +322 627 11 07
E rosa.barcelo@squirepb.com

Ann LaFrance
Co-Chair, Data Protection & Cybersecurity practice, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Andrea Ward
Director, London
T +44 20 7655 1526
E andrea.ward@squirepb.com



Francesca Fellowes
Director, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Asel Ibraimova
Associate, London
T +44 20 7655 1208
E asel.ibraimova@squirepb.com

Emma Yaltaghian
Associate, London
T +44 20 7655 1515
E emma.yaltaghian@squirepb.com

Annette Demmel
Partner, Berlin
T +49 30 72616 8108
E annette.demmel@squirepb.com

Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7583
E stephanie.faber@squirepb.com

2 On 6 October 2020, the CJEU ruled that national legislation that allows for the general and indiscriminate retention of communications data for the purpose of fighting crime is in contravention of the EU law. There are certain conditions that the national legislation must satisfy to meet the principles of EU law. As a result of the ruling, changes may be required to the UK Investigatory Powers Act.