BREXIT AND EUROPEAN DATA PROTECTION - FOR AULD LANG SYNE, MY DEAR!

Date: 20 January 2021

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Alexia Montagnon, Clara Schmit

The European Union (EU) and the United Kingdom (UK) finally came to an agreement on 24 December 2020 (EU-UK Trade and Cooperation Agreement, the Agreement), less than ten days after the European Data Protection Board (EDPB) published a statement on the consequences a no-deal situation would have on the flows of personal data between the EU and the UK (for previous coverage of General Data Protection Regulation (GDPR) and Brexit, please see our alert here). This statement has since been updated on 13 January 2021.

According to this Agreement, until 30 June 2021, any transfer of personal data to the UK will be made under the current framework and will not be considered as a transfer of data to a third-party country. Nevertheless, at the end of this six-month grace period, and unless a compromise is found through an "adequacy decision," the UK will become a third-party country in the eyes of the General Data Protection Regulation no.2016/679. Consequently, all personal data from the EU to the UK will be considered a transfer of personal data outside of the EU, to a country not offering an "adequate level of data protection" from an EU point of view, despite the regulatory framework of the UK remaining the same as it was.

All UK-based companies which would be exchanging data with EU-based companies will need to thoroughly identify such transfers to ensure compliance, as well as on which basis they can be maintained from 30 June 2021 onward.

CONSEQUENCES OF BREXIT ON DATA TRANSFERS FROM THE EU TO THE UK

While the EDPB is currently evaluating whether the UK's regulatory framework could be considered as "adequate" (as per the minute of its 43rd plenary session), such adequacy decision which would allow the free transfer of data between the two blocks is unlikely to be adopted before the Spring of 2021 at the earliest.

In the event where no adequacy decision is taken, the UK's supervisory authority (ICO) recommends all UK-based companies receiving data from the European Economic Area (EEA) to put alternative safeguards in place before the end of April. The possible alternative mechanisms would include:

- Standard Contractual Clauses (SCC), which would remain the most flexible and less time-consuming solution.
    - However, the recent decision from the Court of Justice of the European Union (CJEU) in theFacebook Ireland Ltd. v. Maximillian Schrems case, dated 16 July 2020 (Schrems II, see our alert here) has called for an update to these clauses, and neither the EDPB's recommendations for additional organizational, contractual, and technical measures (here) nor the EU Commission's updated draft SCC will be finalized before 2021.

- Companies wishing to rely on the SCC will therefore need to adopt a flexible and risk-based approach and supplement the now-current SCC with the expected requirements to be finalized.

- Binding Corporate Rules (BCR), which are internal rules that facilitate cross-border data transfers within a multinational group of companies and international organizations.
  - This solution generally requires substantial investment in time and resources for its implementation and only addresses data transfers within an organization, excluding relationships with service providers, for example. They are, however, strongly advised for multi-national companies to streamline the data exchange relating to their internal organization.
- Codes of Conduct, which may be adopted by professional and trade organizations to self-regulate an ecosystem (see our alert here).
  - Just as for BCR, this mechanism would require time and resources. However, this sectoral approach is likely to become more prevalent in the coming years.
- Specific exceptions provided for underArticle 49 GDPR, which would only be relevant for certain situations and not the day-to-day management, as they require the transfer to be:
  - Not repetitive;
  - Relating to a limited number of data subjects'
  - Necessary for the purposes of compelling legitimate interests pursued by the exporting company, not overridden by the interests or rights and freedoms of the data subject;
  - Documented by the exporting organization, with an assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data;
  - Notified to the relevant supervisory authority; and
  - Notified in detail, including the above mentioned legitimate interest, to the data subjects.

Another solution which should be considered would be the joint-controller relationship that would bind the EU-based exporting entity and the UK-based importing entity. Indeed, in such a situation, GDPR should be deemed to apply directly to all the stakeholders involved and the data flows between these entities may not be construed as a “data transfer” per se. While not requiring a specific transfer mechanism, this relationship will need to be governed by a dedicated joint controllership agreement, and the parties thereto will be jointly and severally liable.

Meanwhile, and as of the time of this writing, the UK Government has stated that they would recognize the EU as an importing destination offering an adequate level of protection. Therefore, companies who data is only being transferred from the UK to the EU would have no additional requirements.

THE END OF THE ONE-STOP-SHOP AND REPRESENTATIVE APPOINTMENTS

The One-Stop-Shop mechanism (OSS), which establishes one EU supervisory authority as competent for administering situations involving the processing of personal data over several EU Member States, has not been included in the Agreement. As a consequence, as of 1 January 2021, UK entities not otherwise subject to GDPR

will no longer benefit from this mechanism. This will notably impact the management of personal data breach notification (see our analysis of the impact on personal data breach here).

Both the EDPB and its UK counterpart, the ICO, have stated they would be working in close cooperation to ensure a transition as seamless as possible to all affected stakeholders, including for cases which are currently being investigated.

UK companies must now consider whether another supervisory authority may have jurisdiction over their data processing operations in the EU. Such jurisdiction may result from:

- Their establishment within the EU, e.g. through a branch, subsidiary, or any other stable arrangement, as per Article 3.1 GDPR.
    - To be considered an "establishment" under GDPR, however, the EU-based corporate offshoots from a UK company would need to be directly involved in the data processing operations at stakes, or inextricably linked to the activities of the UK company. A case-by-case review will therefore be required.
- Where no such establishment exists, their activities, i.e. (i) the offering of products and services to EU data subjects per (ii) the monitoring of their behavior taking place in the EU, as per Article 3.2 GDPR.
    - In that situation, the oft-overlooked Article 27 GDPR requires UK companies to appoint a representative in the EU as of 1 January 2021. This representative may be addressed by supervisory authorities and data subjects alike on all issues related to processing activities in order to ensure compliance with GDPR. It remains unclear at this stage whether this representative could be expose to a subsidiary liability for the entity they represent, as Recital 80 GDPR provides that "*The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*", but such situation is not detailed within the articles of GDPR.
    - Note that the designation of such a representative would still be required for the joint-controller not established within the EU as detailed above.

The K&L Gates Data Protection team remains available to assist you in achieving compliance of your data transfers at a global level. Please get in touch if you would like to discuss the steps that your organization might want to consider to prepare now for the end of the transition period.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

