December 29, 2020

Brexit, Data Protection and International Data Transfers in 2021

On 24 December 2020, EU and U.K. representatives agreed on a new trade deal. This last-minute deal has avoided a potentially disruptive “no deal” situation, which would have had significant implications for international data transfers in addition to the broader impact on trade in goods and services between the U.K. and EU.

The U.K. left the EU on 1 January 2020. Since then, there has been a twelve-month transition period, ending on 31 December 2020, during which time EU laws continue to apply. Now that the transition period is coming to an end, U.S. businesses with operations in the EU and the U.K. will need to make a number of operational adjustments.

In respect of international data transfers, the new trade deal creates a “specified period” from the date of entry into force of the trade agreement that will continue for four months and can be extended to six months if the U.K. and EU agree. During this period, transfers of personal data from the European Economic area (the EU countries together with Norway, Iceland and Liechtenstein) to the U.K. will not be considered to be transfers to a “third country,” which would require specific safeguards. This effectively retains the status quo until the European Commission adopts an “adequacy decision” that will designate the U.K. as one of the territories that the EU recognizes as offering an equivalent level of protection for personal data as EU law. During the specified period (effectively a further transition period in respect of data protection laws), the U.K. must not make any changes to its data protection regime, in particular the international data transfer provisions, without the agreement of the EU. Talks around the adequacy of the U.K.’s data protection framework under Article 45 of the EU’s General Data Protection Regulation (GDPR) have been running in parallel to the trade talks. While they are partly a technical legal exercise, they have also been part of the broader political and economic negotiations. They are subject to their own procedural requirements, including an opinion from the European Data Protection Board. The specified period gives some breathing space for this process to continue.

We set out below a brief summary of data transfer arrangements and broader implications of the end of the transition period on 31 December 2020.

1. U.K. to EU Data Transfers

Data transfers from the U.K. to the EU will not be affected, and personal data can continue to flow freely. The U.K. has legislated under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 (the "**DPPEC Regulations**") — which amend the Data Protection Act 2018 and the U.K. GDPR (which is the GDPR as retained in U.K. law by section 3 of the European Union (Withdrawal) Act 2018) — to provide that any EEA member state will be regarded as providing an adequate level of data protection such that personal data can be transferred to such member state without adopting an appropriate safeguard (such as, for example, standard contractual clauses). Therefore, for example, a U.S. company with subsidiaries in the U.K. and in the EU may continue to transfer personal data from the U.K. to sister companies in Germany or Italy.

2. EU to U.K. Data Transfers

Pending the adequacy decision noted above, during the four to six month specified period, data transfers from the EU to the U.K. can continue as before. Had a trade deal not been agreed upon, the U.K. would have immediately become a "third country" for the purposes of the GDPR, and transfers of personal data from the EU to the U.K. would have had to be carried out using an appropriate safeguard under Article 46 — for example, standard contractual clauses or binding corporate rules. This provides some relief for U.S. businesses with operations in a number of European countries, which shared, for example, personal data relating to employees or customers between its EU entities and U.K. operations.

3. U.K. to Non-EU Data Transfers:

Adequacy decision countries: Data transfers from the U.K. to those countries and territories that benefit from an EU Commission adequacy decision will not be affected, and personal data can continue to flow freely. The U.K. has adopted the EU Commission's existing decisions under Schedule 21, Part 3 of the Data Protection Act 2018. These countries and territories are Gibraltar, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Faroe Islands, Andorra, Israel, Uruguay, New Zealand and (most recently) Japan.

"Third" countries (i.e., those countries which do not benefit from an adequacy decision): The position remains the same in respect of data transfers from the U.K. to third countries. Any transfers of personal data from the U.K. to such countries must be carried out using an appropriate safeguard — for example, standard

contractual clauses or binding corporate rules. The U.K. has legislated under the DPPEC Regulations to recognize the existing European Commission-approved standard contractual clauses as providing an appropriate safeguard for restricted transfers out of the U.K. Moreover, following the decision in *Schrems II* (see "EU Court Issues Landmark Ruling on Transfer of Personal Data Outside European Economic Area"), EU data exporters should carry out a data transfer impact assessment and, if necessary, implement additional safeguards to ensure that the personal data transferred will be subject to a standard of data protection equivalent to that provided in the EU. (See further our previous alert, "European Data Protection Board Issues New Recommendations for International Data Transfers: Essential Guarantees, Supplemental Measures, and False Warrant Canaries.")

Therefore, while additional complications have been avoided, for the time being, in respect of transfers of personal data from EU entities to the U.K., implementing appropriate safeguards for transfers of personal data from the U.K. or EU to the U.S. must remain high on the agenda for U.S. businesses in 2021.

4. Regulatory Overlap

There will now be two separate and distinct versions of the GDPR which may apply to organizations: the U.K. GDPR (i.e., the GDPR as incorporated into U.K. law but as revised to reflect the fact that the U.K. is no longer an EU member state) and the EU GDPR (i.e., the GDPR as directly applicable in all EU member states). At least to begin with, the data protection standards set by the U.K. GDPR and EU GDPR will be essentially the same. However, over time, there is scope for regulatory divergence (within the confines of an adequacy decision). Furthermore, as they are distinct laws with separate regulators, organizations that are subject to both the U.K. GDPR and the EU GDPR (i.e., under the extraterritorial application limbs set out in each statute — see **Extraterritorial scope** below) face separate regulatory requirements and enforcement procedures. We summarize some of the more significant aspects of the dual and overlapping regulatory regimes below.

- **Identity of regulator:** For organizations subject to the U.K. GDPR, that organization's data protection regulator will be the U.K. Information Commissioner's Office (the " **ICO**"). For organizations subject to the EU GDPR, that organization's regulator will be the supervisory authority in the relevant EU member state.
- **Extraterritorial scope:** An organization established in the U.K. (but not in any other EU member state) will be subject to the U.K. GDPR. However, it may also be subject to the EU GDPR under the EU GDPR's extraterritoriality limbs. That is, because that U.K. organization either (a) offers goods and services to data subjects in the EU, or (b) monitors the behaviour of data subjects in the EU. For example, if a U.S. manufacturer has a U.K. subsidiary, it will be subject to the U.K. GDPR. If that U.K. subsidiary also sells into the EU market (for example, by actively marketing to customers in France or Germany) it will also be subject

to the EU GDPR. Similarly, the converse may also be true in respect of organizations established in the EU (but not in the U.K.) but which offer goods and services to, or monitor the behaviour of, U.K. data subjects. In this case, that EU organization will be subject to the EU GDPR by virtue of its establishment but also be subject to the U.K. GDPR under the U.K. GDPR's extraterritoriality limbs. While the practical differences in regulatory compliance may be minimal (except for the immediate requirement to ensure that the appropriate representatives have been appointed — see further below), businesses will have to monitor two different regulatory regimes.

- **Lead supervisory authority:** For organizations for which the ICO was their lead supervisory authority under the EU GDPR, this will no longer be the case under the EU GDPR (assuming that organization is also subject to the EU GDPR). Affected organizations must consider: (a) whether there is an alternative EU member state supervisory authority that could instead serve as their lead supervisory authority; or (b) whether they are no longer able to benefit from the "one stop shop" procedure under the EU GDPR (Articles 56 and 60 to 62) and, if so, consider which supervisory authority (or authorities) are likely to have jurisdiction to investigate any complaints or alleged breaches of the EU GDPR. Therefore, for example, a U.S. business with its European head office in the U.K., but with sales and marketing operations in France, Germany and Spain, and HR functions in the Netherlands will need to consider which of its EU operations will be its main establishment in respect of its data protection compliance.
- **Representatives:** U.K. organizations that are subject to the EU GDPR, but not established in the EU, (i.e., are subject to the EU GDPR under its extraterritorial limbs) will need to appoint an EU representative under Article 27 of the EU GDPR. EU organizations not established in the U.K. but subject to the U.K. GDPR under its extraterritorial limbs will, similarly, need to appoint a U.K. representative under the equivalent provisions of the U.K. GDPR.
- **Cooperation with supervisory authorities:** Under both the EU GDPR and the U.K. GDPR, organizations must engage (in certain circumstances) with relevant supervisory authorities in connection with data breach notifications for the appointment of a data protection officer and before engaging in high-risk processing. Where the relevant processing is cross-border (affecting the EU and the U.K.), organizations will now need to engage independently with both the U.K.'s ICO and relevant EU supervisory authorities.

5. Other Considerations:

Organizations must now also review and consider whether privacy notices, data impact assessments and data protection officer appointments need to be revised and updated as a result of the U.K. becoming a third country for the purposes of the EU GDPR and its associated effects, particularly around data transfers.

MEET THE AUTHORS

Huw Beverley-Smith

Partner

+44 (0) 20 7450 4551
London
huw.beverley-smith@faegredrinker.com

Jonathon A. Gunn

Associate

+44 (0) 20 7450 4512
London
jonathon.gunn@faegredrinker.com

Services and Industries

Intellectual Property

Technology Transactions & Licensing

International Transactions

Government & Regulatory Affairs

Privacy, Cybersecurity & Data Strategy

Customs & International Trade

International Team