UK data protection law in the post-Brexit world

Published 02-Jul-2019 by
Mark Young, Jack Boeglin and Sam Jungyun Choi

Notwithstanding lingering uncertainty as to when, how, and if Brexit will ultimately take place, the UK government has clarified the state of UK data protection law in the aftermath of Brexit.

Earlier this year, the UK government issued two sets of regulations aimed at readying UK data protection law for a post-Brexit world. The key takeaway from these regulations and the relevant guidance is that UK data protection law will in many respects remain undisturbed by Brexit, regardless of whether a departure deal with the EU is reached. However, organizations that process personal data of individuals in the European Economic Area (EEA) should continue to monitor for further updates on the status of international data transfers.

These regulations, which were made pursuant to the EU (Withdrawal) Act 2018 (EUWA), will only come into force in most respects upon the UK's withdrawal from the EU. Broadly speaking, these regulations are intended to preserve the status quo post-Brexit by:

- amending certain provisions of the General Data Protection Regulation (GDPR) to allow it to be retained as UK domestic law; and
- transitionally adopting certain key decisions of the EU institutions that, collectively, would allow for the continued lawfulness of personal data flows out of the United Kingdom where currently permitted under EU law.

In both regards, these regulations are consistent with prior guidance from the UK Government.

The bulk of the first set of regulations — The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 — is dedicated to localising the GDPR into UK domestic law. Following the UK's departure from the EU, certain language in the GDPR — for instance, that requiring consultation of, or affording decision-making authority to, the European Commission or European Data Protection Board — will no longer be appropriate in a purely domestic context. These regulations therefore re-assign powers afforded to EU institutions under the GDPR to UK equivalents and substitute EU-specific language in the GDPR with UK-appropriate terms (e.g., replacing "GDPR" with "UK GDPR").

Although many of these localisations are semantic, some impose new requirements on entities that process UK personal data. Perhaps most notably, entities outside of the UK that process the personal data of UK data subjects must appoint an Article 27 representative in the UK post-Brexit, except where any processing is occasional, low risk, and does not involve special category or criminal offence data on a large scale. For many organizations, this will mean maintaining separate representatives in the UK and the EU. Another substantive impact would be in relation to personal data breach notifications.

These regulations also provide for the transitional adoption of certain European Commission decisions (1) declaring that particular third countries provide an adequate level of data protection or (2) approving the language of particular standard contractual clauses. The Binding Corporate Rules that the UK Information Commissioner's Office (ICO) approved pre-Brexit will still be able to be used to legitimise transfers outside of the UK. (These regulations do not, however, provide for the ongoing adoption of data protection decisions from the EU institutions post-Brexit; in other words, should the European Commission deem a third country to provide an adequate level of data protection following the UK's withdrawal from the EU, that country will need to receive an independent adequacy determination from the UK before the free flow of personal data from the UK to that country will be permissible).

The second set of regulations — The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019 — supplement the first set of regulations with respect to the EU-U.S. Privacy Shield.

These secondary regulations will require Privacy Shield-certified companies in the U.S. to include in their privacy policies a commitment to complying with Privacy Shield principles with respect to UK-originating personal data post-Brexit. While compliance with these regulations may require such companies to modify their privacy policies, the regulations are not intended to impose any new substantive requirements.

To be clear, neither set of regulations provide, nor could they provide, for the lawfulness of data flows from the EEA into the UK post-Brexit. Unless and until the European Commission deems the UK to provide an adequate level of data protection, therefore, companies intending to import data from the EEA into the UK post-Brexit will need to put in place alternative transfer safeguards, such as Standard Contractual Clauses.

The ICO has issued updated guidance on international data transfers post-Brexit.

The issue of Brexit is not the only moving target on the topic of international data transfer rules. Both the EU-U.S. Privacy Shield and the Standard Contractual Clauses are under challenge in European courts. Organizations relying on either mechanism to legitimize international transfers should monitor upcoming developments closely.

Produced by Thomson Reuters Accelus Regulatory Intelligence 02-Jul-2019

THOMSON REUTERS™