

The future EU-UK relationship: options in the field of the protection of personal data for general processing activities and for processing for law enforcement purposes

Study by PwC, time.lex and Spark Legal Network

The aim of this study was to briefly examine possibilities and legal and institutional prerequisites for continuing the exchange and processing of personal data between the UK and the EU following Brexit, also in view of a future relationship agreement. This was done, by looking at the existing legal mechanisms and policy measures presently used to support the information flows between the EU and UK, and between the EU and third countries. We also investigated the data processing mechanisms in seven European Commission DGs and in eight EU agencies.

The study showed that, while there are currently legal and policy measures in place to support the flow of personal data between the EU and a third country, none of these (in isolation or collectively) would be sufficient to permit a continuation of personal data flows and cooperation in relation to data protection on the same basis as today.

Notably, this includes an affirmative adequacy finding for the UK (in relation to data protection in general under the GDPR¹ and in relation to law enforcement under the Law Enforcement Directive)². This is an appropriate solution for private sector exchange. However, although it may contribute to ensuring a continued integration of the UK in personal information exchanges, it will not be sufficient for public sector exchange because a multitude of legal instruments exist beyond general data protection law, that determine which countries may participate in information exchanges, and on which basis. An adequacy finding would thus need to be complemented by a broader legal basis in the form of a legal agreement that would authorise the UK and EU to continue to participate in information exchanges. Furthermore, an adequacy decision requires a lengthy process which could only begin once the UK has left the EU. An adequacy finding is thus insufficient to avoid a temporary standstill in information exchanges.

Other common legal instruments used in data protection law to organise personal data exchanges, such as standard contractual clauses, binding corporate rules, certification, codes of conduct and approved ad hoc contractual agreements. However, the use of such instruments is resource intensive and unsuitable to set up a broad framework for data exchanges that can be used to organise compliance transfers of personal data on a large scale (such as by SMEs).

Provided that there is a consensus on the need for continuity in existing personal data exchanges between the EU and the UK, and for continued alignment between data protection law and data protection policy between the EU and the UK, a bespoke instrument is required that establishes an initial standstill period that allows the EU and the UK to continue personal data exchanges on a provisional basis, taking into account that the UK's data protection law is already substantially aligned to EU data protection law and policies. Furthermore, the bespoke agreement can allow the UK to participate in (i) the development of common EU data protection policy (i.e. by contributing to positions of the European Data Protection

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Board, by participating in the one-stop-shop mechanism, and by ensuring a homogeneous application of EU case law in relation to data protection, including in the UK), (ii) internal market data transfers, and (ii) security and law enforcement initiatives. Assuming that the EU and UK mutually agree on the desirability of these priorities, this would seem to be the only approach that can avoid a temporary halt in personal data exchanges, and that can ensure continuous alignment of data protection policy between the UK and EU, even after Brexit.