ARTICLE

THE IMPACT OF BREXIT ON DATA TRANSFERS TO THE UK FROM THE EUROPEAN UNION

IT and Data Protection Competition, Retail and Consumer Law Commercial and International Contracts | 10/02/21 | Florence Chafiol

PROTECTION DES DONNÉES PERSONNELLES

The EU-UK Trade and Cooperation Agreement creates a transitional period of four months (possibly six months) from January 1, 2021 to allow the European Commission a further period to carry out a formal assessment of the adequacy of UK data protection legislation under Article 45 of the GDPR. UK companies without an establishment in the EU have nevertheless lost the benefit of the one-stop-shop mechanism.

Brexit still in transition

Following the referendum on the United Kingdom's withdrawal from the European Union voted on June 23rd, 2016, and after years of negotiations, the European Union and the United Kingdom have finally reached a withdrawal agreement, applicable from January 1, 2021.

Within the framework of this agreement, and in order to organize the modalities of future cooperation between the European Union and the United Kingdom, a Trade and Cooperation Agreement was concluded on December 24, 2020[1].

The United Kingdom is no longer a Member State of the European Union and would therefore no longer be subject to European directives and regulations, including the famous General Data Protection Regulation (the "**GDPR**").

However, the Trade and Cooperation Agreement provides for a transitional period of four months, which may be extended to six months under certain conditions; during this period, "*the transfer of personal data from the Union to the United Kingdom shall not be considered as a transfer to a third country under Union law**[2]**"*. The purpose of this transitional provision is to allow more time for the European Commission to issue an adequacy decision regarding the UK data protection legislation. The aim of this approach is to avoid the need for stakeholders to provide, at least temporarily, for appropriate safeguards to regulate transfers of personal data to the UK in accordance with Chapter V of the GDPR (such as the standard contractual clauses, themselves subject to an update by the European Commission, and challenged following the Schrems II judgment of July 16, 2020 of the European Court of Justice (the "ECJ")[3], or the Binding Corporate Rules (or *BCR*)). It is important to note that the United Kingdom has already adjudged that the personal data protection laws of the EU Member States, the member states of the European Economic Area ("EEA") and Switzerland are adequate. A reassessment of this adequacy is scheduled to take place in four years' time.

Therefore, depending on the outcome of this transitional period, different solutions will be available to those subject to the GDPR who transfer personal data to the United Kingdom. In addition, Brexit marks the end of the "one-stop-shop mechanism", a provision on cooperation between the lead supervisory authority and other supervisory authorities concerned, provided for in the GDPR, for UK companies without a principal place of business in the European Economic Area, as of December 31, 2020. Indeed, this mechanism does not benefit from the new transitional period.

Solutions for personal data transfers to the UK

The most preferable: the adequacy decision. The transitional period potentially applicable until July 1, 2021 has been decided to allow the European Union to carry out an assessment of the UK legislation (the "*UK GDPR")* in order to issue or not, a decision on adequacy with regard to the United Kingdom on matter of personal data protection. Indeed, a UK adequacy decision will immediately end the current transitional period.

An adequacy decision will have to demonstrate that the *UK GDPR* provides equivalent protection for personal data to that which existed when the United Kingdom was subject to the GDPR.

In this respect, the United Kingdom would join the other twelve countries recognized as offering adequate protection for personal data (Andorra, Argentina, Canada (subject to conditions), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay).

However, while the adoption of such an adequacy decision seems to be the most preferable mechanism to regulate the transfer of personal data between the European Union and the United Kingdom, some criticisms have been made about the compliance of UK surveillance laws with the GDPR, which could be considered too intrusive to allow for an adequacy decision. In the "Schrems II" decision, the ECJ invalidated the existing transfer mechanism between the European Union and the United States based on the Privacy Shield and held that "the *requirements of US law, and in particular certain programs allowing access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data that are not restricted so as to meet requirements substantially equivalent to those required by EU law, and that such legislation does not provide data subjects with rights of legal action before the courts against the U.S. authorities **[4]***". UK surveillance legislation is similarly criticized, which the European Commission is likely to consider in its assessment.

In the absence of an adequacy decision by the European Commission at the end of this maximum six-month transitional period, any transfer of personal data to the United Kingdom will be considered as a transfer to a third country and will have to be subject to the safeguards provided for in Chapter V of the GDPR.

Standard contractual clauses. The use of the standard contractual clauses adopted by the European Commission (the "SCCs") is one of the guarantees considered "appropriate" under Chapter V of the GDPR. They take the form of a contract between the European data exporter and the data importer established in a third country.

This model clauses are currently being revised to consider the consequences of the Schrems II decision of the ECJ.

Indeed, the ECJ has confirmed the validity of the mechanism of standard contractual clauses to regulate the transfer of personal data outside the European Union, subject to two new constraints:

- A case-by-case analysis of the legislation of the country of destination of the data for any transfer must be carried out by the exporter, to determine:

  - the level of protection provided in the third country concerned, or
  - if the legislation of the third country undermines the effectiveness of the legal instruments concerned (SCCs).

- If this assessment shows that the effectiveness of the legal instruments concerned is being undermined (which is clearly the case in the United States and is a matter of concern regarding UK legislation), additional measures must be put in place.

- Finally, if the combination of additional measures and SCCs does not ensure that the appropriate safeguards are respected:

  - the data exporter is then required to suspend or terminate the transfer; or
  - if the data exporter still wishes to proceed with the transfer despite failure to comply with the appropriate guarantees, it must notify its competent supervisory authority (in France, the CNIL).

The question of the effectiveness of these SCCs concerning data transfers to the United Kingdom could nevertheless be called into question, in view of the criticisms raised concerning the UK surveillance legislation. Indeed, there are currently no additional measures on which there is a consensus and which would make it possible to prevent access to personal data by the authorities of the country receiving the data in a certain and effective manner.

BCRs. Binding corporate rules known as "*BCRs*" correspond to the internal rules relating to transfers of personal data to third countries within the same group of companies. These rules, subject to prior authorization by the lead supervisory authority, are an effective compliance tool. Nevertheless, the same issue concerning SCs affects BCRs: indeed, the possibility to transfer personal data on the basis of BCRs will depend on the result of the assessment that the data exporter must make, taking into account the circumstances of the transfer and the additional measures that it could put in place. These additional measures as well as BCRs, after a case-by-case analysis of the circumstances surrounding the transfer, should ensure that the legislation of the third country does not conflict with the level of protection afforded by these tools.

Finally, the European Data Protection Board (the "EDPB") specified in an information note dated July 22, 2020 that at the end of the transitional period of December 31, 2020, the UK data protection authority, the Information Commissioner's Office, (the "ICO"), would lose any competence it had under the GDPR in relation to the BCRs. Therefore, each group of companies whose BCRs have been approved by the ICO would have to designate a new competent EEA supervisory authority before December 31, 2020 which would be responsible, following an opinion from the EDPB, for issuing a new decision approving those BCRs. If the transition had not been made before December 31, 2020, groups of companies will not be able to rely on their BCRs as a valid transfer mechanism for data transfers outside the EEA after the end of the transition period[5].

Codes of conduct and certification are also possible guarantees for international transfer of personal data.

Finally, derogations to such guarantees are provided for in Article 49 of the GDPR but are to be strictly interpreted.

End of the one-stop shop mechanism for UK companies without a principal place of business in the European Economic Area

End of the one-stop shop mechanism.

The one-stop-shop mechanism, a cooperation mechanism relating to data protection, aims to facilitate cooperation between European supervisory authorities. This mechanism is available to companies (controller or processor) (i) with establishments in several EU Member States or (ii) which process the personal data of persons residing in several EU Member States. This mechanism then allows the companies concerned to have only one interlocutor for compliance with the GDPR, the lead supervisory authority.

This lead authority, that of the country in which the company's principal place of business is located, must cooperate with the other data protection authorities concerned by the cross-border data processing carried out by the company. The lead authority will have to coordinate the joint decision-making with regard to the processing operations in question. The supervisory authorities of each member state concerned may thus take up a European case of cross-border processing and issue a single decision harmonized and coordinated with the common European policy on the matter, which will then apply throughout the Union.

Following Brexit, and since January 1, 2021, the ICO is no longer considered as lead authority, as the transitional period of four (or six) months opened by the Trade and Cooperation Agreement is not applicable to this procedure.

Thus, while the legal framework for the protection of personal data remains unchanged for data subjects and companies during this additional period, the potential issues related to the processing of personal data between the UK and EU Member States will no longer be dealt with by the same lead authority. Only UK data controllers or processors with a principal place of business established in the European Economic Area can continue to benefit from the one-stop-shop mechanism, by designating a new lead authority to the supervisory authority of their principal place of business within the EU.

The CNIL indicated that the European supervisory authorities "*have been in contact with the ICO over the last few months to allow an orderly transition to this new situation, ensuring that the EU authorities follow a coordinated approach in dealing with existing complaints and cross-border cases involving the ICO, in order to minimize possible delays and inconvenience for the plaintiffs concerned.* »

The reciprocal obligation to appoint representatives.

Since January 1, 2021, UK data controllers and processors whose processing activities are subject to the GDPR, under Article 3, must designate a representative within the European Union.

Thus, if a UK company, having no establishment, within the meaning of European case law, within the European Union, processes personal data in connection with (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or (ii) the monitoring of the behavior of data subjects in the Union, as far as their behavior takes place within the EU, then that company will have to appoint a representative within the EU, in accordance with Article 27 of the GDPR, except in certain limited cases (Article 27-2).

The same applies to European companies, not having an establishment in the United Kingdom, and meeting the same conditions in terms of processing activity (offering goods or services to people in the United Kingdom or monitoring the behavior of individuals in the United Kingdom); they will also have to appoint a representative in the United Kingdom.

[1] *"Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part*".

[2] Article FINPROV.10A: Provisional provision on the transmission of personal data to the United Kingdom

[3] CJEU 16 July 2020, CPP v. Facebook Ireland Ltd and M. Schrems, case C-311/18

[4] https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-premieres-questions-reponses-du-cepd

[5] EDPB - Information note on BCRs for Groups of undertakings /enterprises which have ICO as BCR Lead SA (July 22, 2020).