International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838; Print ISSN: 2664-682X; Impact Factor: RJIF 5.42
Received: 22-01-2021; Accepted: 12-02-2021; Published: 03-03-2021
Volume 3; Issue 1; 2021; Page No. 19-27

Brexit, international private relations and personal data protection, after the new association agreement EU-United Kingdom

Alfonso Ortega Giménez
Contracted Doctor, Private international Law, Miguel Hernández University of Elche, Spain

Abstract
On 31st January 2020, the United Kingdom formally left the European Union. However, by virtue of the Withdrawal Agreement signed, the United Kingdom has ceased to be a member of the European Union but must continue to apply the General Data Protection Regulation (GDPR) in matters of personal data protection, to all data of data subjects outside the United Kingdom, that have been processed prior to the end of the transitional period (which ends, a priori, on 31st December 2020). This implies that, for the purpose of exporting data, the situation in the United Kingdom is comparable to that of a Member State, so that during the transition period the current GDPR is applicable; However, the situation will be completely different after the end of the transition period that will require both the United Kingdom and the European Union to prepare a new generation legal framework to meet the challenges in terms of personal data protection that the Current globalised environment demands, which will have the projected New Association Agreement between the European Union and the United Kingdom as a reference.

Keywords: Brexit, United Kingdom, data protection, international data transfer

Introduction

Approach

Since 31st January 2020, the United Kingdom is no longer a member State of the European Union. And, "shortly", the United Kingdom will be deemed to be a "third country" with regard to personal data protection. In accordance with the provisions of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, signed in Brussels and London on 24th January 2020 (henceforth, the Withdrawal Agreement) [1].

The departure of the United Kingdom from the European Union represents a change to all the economic and social aspects, and, with regard to personal data protection, it means that: personal data transfers from the European Union will be subject to greater restrictions, which will affect both service providers as well as companies that transfer personal data of clients or workers to their parent companies or subsidiaries located in the United Kingdom. Thus, in the absence of a specific agreement, from the withdrawal date (= 1st January 2021), the rules regarding international data transfers to third countries will apply. Notwithstanding, it is foreseeable that the Commission grants the United Kingdom "secure country" status given that it would inherit the regulations in force until now, bearing in mind that the United Kingdom was one of the first countries of the European Union to adapt its internal regulations to the demands of Regulation (EU) 2016/679 of the European Parliament and Council of 27th April 2016 regarding the protection of physical persons with respect to the processing of personal data and the free circulation of these data, whereby repealing Directive 95/46/CE (henceforth, the GDPR) [2]. In this sense, the United Kingdom has made it clear that the GDPR will be "absorbed" into United Kingdom law; however, organisations that depend on international transfers of personal data between the United Kingdom and the European Economic Area (henceforth, the EEA) may be affected since personal data has been allowed to flow freely between organisations in the United Kingdom and the European Union without any specific measures. Even if the Commission grants "secure country" status, there may be a time lapse between the definitive separation from the European Union and the Decision of the Committee to deem the United Kingdom to be a "secure country", in which case any data movements that may take place during this period could entail an "international data transfer"; and, therefore, for example, companies that contract data processing or hosting services in the United Kingdom may need to regularise these transfers for an indefinite period of time. It is also possible that the European Union reacts to Brexit "vindictively", and that, among the many obstacles that it puts in the way of the United Kingdom is not recognising it as a "secure country". In this event, it would degenerate into a de facto blockade similar to the one we have been suffering since October 2015, when the Safe Harbour Agreement with the United States was cancelled [3].

Legal system for personal data protection in the United Kingdom after Brexit.

There will be many legal consequences caused by Brexit coming into force. With regard to the scope of personal data protection,

[1] DOUE L 29/7 of 31st January 2020.
[2] DOUE L 119/2 of 4th May 2016.
[3] *Vid.* ORTEGA GIMÉNEZ, Alfonso and GONZALO DOMENECH, Juan José, "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido Un "país seguro"? (Brexit and personal data protection: will the United Kingdom cease to be a "safe country"?), in *Revista Aranzadi Unión Europea*, *núm.* 11/2019, Editorial Aranzadi, S.A.U., 2019, pp. 1-23.

the consolidation of Brexit establishes that the United Kingdom will be deemed to be a "third country", obliging the United Kingdom to "transform" its legal system for personal data protection to face the "new panorama".

Regulatory framework for personal data protection in the United Kingdom.

The United Kingdom currently has national regulations regarding personal data protection that are already adapted to the GDPR; with regard to data protection, the British have adopted an innovative and flexible approach, seeking a balance, which is not at all easy, between legal demands and requirements on the one hand and, on the other, technological reality [4]. They have thus been pioneers in recognising the two sides of the same coin, merging the fundamental right to data protection with the right to access public information.

Another contribution to the field of data protection coincides with the creation of the *Data Protection Tribunal*, an independent body that specialises in data protection and the right to access information whose mission is to resolve appeals made to the British data protection authority, in other words, the *Information Commissioner's Office* [5]. Finally, the use of codes of conduct has been encouraged now for several decades (a policy that has been transferred to the GDPR). Even though article 50 of the TEU has already been activated, the British have not ceased in their efforts to adapt to the GDPR: thus, in 2018, a new Data Protection Law, the *Data Protection Act 2018*, was passed in 2018, whereby repealing the previous one of 1998 and whereby the United Kingdom intends to adapt to the current requirements of the GDPR. Subsequently, the *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* which, making use of the powers of the *European Union (Withdrawal) Act 2018*, was issued in order to adapt certain European provisions to British law. Specifically, it was decided to adopt the GDPR as its own law: the *United Kingdom General Data Protection Regulation* (UK GDPR).

Data Protection is similar to European Union data protection Law. The United Kingdom aspires to maintaining a harmony of material solutions between European and internal regulations with respect to personal data. And the reason? Beyond the complexity that Brexit brings with it, to achieve equality between both regulatory blocks (European *vs.* British), preventing distortions of the market and the rights of citizens in a strategic sector with huge repercussions [6].

All these considerations enable us to affirm that the United Kingdom maintains a firm commitment to the recognition of this fundamental right, which they could justify when the time comes to recognise an adequate level of protection; even to not be considered a "third country", but to analyse other possible means of facilitating the flow of data without resorting to instruments envisaged for international personal data transfers [7].

Legal system for personal data protection according to the Withdrawal Agreement between the United Kingdom and the European Union.

It is well known that, on 25th November 2018, the 27 Member States of the European Union endorsed the Withdrawal Agreement project and approved the Political Declaration on future relations between the European Union and the United Kingdom project. On 5th December of the same year, the European Commission started the procedure for the signing and execution of the aforementioned Withdrawal Agreement between the United Kingdom and the European Union. On 13th December, the leaders of the European Union held an extraordinary meeting of the European Council, in its composition of article 50, to debate Brexit. At this meeting, they again confirmed their Conclusions of 25th November, when they endorsed the Withdrawal Agreement and approved the Political Declaration. On 11th January 2019, the Council adopted a firm decision on the Withdrawal Agreement, and a project for the Decision regarding the execution of the Withdrawal Agreement was also approved; and it was decided to send said project for the Decision to the European Parliament for its approval [8].

It is thus necessary to analyse the provisions that the Withdrawal Agreement establishes regarding the fundamental right to data protection (=Title VII of the Agreement, specifically in articles 70 to 74).

Article 70 establishes that it should be understood as "Union Law on personal data protection"; including the GDPR, among other regulations [9].

It is article 71 that specifically regulates what occurs with the processing of personal data from data subjects outside the United Kingdom. In this sense, the precept indicates that European Union Law will be applied to the matter provided that: a) The personal data were processed by virtue of Union Law in the United Kingdom before the end of the transition period, in other words, from 31st December 2020; or, b) The personal data were processed in the United Kingdom after the end of the transition period based on this Agreement [10].

---

[4] *Vid.* SARMIENTO, D., "Y después del Brexit… ¿Qué?" (And after Brexit… What?), in *El Cronista del Estado Social y Democrático de Derecho, núm.* 64, p. 42.

[5] The Information Commissioner's Office is a public body with powers to inspect and sanction since long before the GDPR came into force and has been applied.

[6] *Vid.* "Brexit y la protección de datos personales: incógnitas e incertezas" (Brexit and data protection: unknowns and uncertainties), in: http://www.legaltoday.com/blogs

[7] *Vid.* DE HERT, P., and PAPAKONSTANTINOU, V., The rich contribution to the field of EU data protection: Let's not go for third country *status* after Brexit, in *Computer Law & Security Review*, Nº 33, 2017, p. 357.

[8] *Vid.* CORRAL SASTRE, A., "Las transferencias de datos personales al Reino Unido en la era postbrexit" (Personal data transfers to the United Kingdom in the post-Brexit era), in *Diario la Ley*, Especial Revista de Derecho Digital e Innovación, Nº 3, 2019, p. 14.

[9] Article 70. Definition

For the purposes of this title, it will be understood as «Union Law regarding personal data protection »:

a. Regulation (EU) 2016/679, except for chapter VII;
b. Directive (EU) 2016/680 of the European Parliament and Council (90);
c. Directive 2002/58/EC of the European Parliament and Council (91);
d. Any other provisions of the Union Law that regulate personal data protection.

[10] Article 71. Personal data protection

a. Union Law regarding personal data protection will be applied in the United Kingdom with respect to the processing of the personal data of data subjects outside the United Kingdom provided that the personal data: a) have been processed according to Union Law in the United Kingdom before the end of the transition period; or b) are processed in the United Kingdom after the end of the transition period based on this Agreement.
b. Section 1 will not be applied in so far as the processing of personal data considered therein is subject to an adequate level of protection by virtue of the provisions of the decisions that are applicable pursuant to article 45,

We can therefore indicate that, based on the Withdrawal Agreement, European Union Law will continue to be applied with regard to the protection of all personal data obtained before 31st December 2020 since the GDPR is the data protection legislation in force in the United Kingdom. After this period, the processing of personal data from data subjects from outside the United Kingdom will adhere to the provisions of the Agreement, which indicates nothing about the legislation applicable beyond what is indicated in article 134 regarding financial provisions [11]. In other words, after the transition period established in the Withdrawal Agreement, and unless this establishes something else, the personal data processed will be governed by British legislation, in other words, for now, the *Data Protection Act 2018*.

Section 2 of article 71 foresees the possibility of the Commission issuing a decision on the adequacy of the level of data protection in the United Kingdom, such that the provisions of section 1 of the aforementioned article would not be applicable because any data flow would be covered by the adequacy decision. In fact, the *Data Protection Act 2018* is an adaptation to EU regulations, which mentions the GDPR as a benchmark regulation in this matter, assuming, therefore, that it will be applied.

The Withdrawal Agreement includes, in its article 72, confidential processing and restricted use of data and information in the United Kingdom [12]; article 73 refers to the processing of data and information obtained from the United Kingdom [13]; and, finally, article 74 includes what relates to information security [14].

The general principle of transfers and adequacy decisions as the main instrument for international data transfers.

The principle considered in the application regulations determines that international data transfers may only be made to a third country or international organisation if: a) It complies with all obligations relating to processing included in the applicable regulations; and b) It ensures sufficient guarantees when it comes to making an international transfer, especially those consisting of guarantees in subsequent transfers.

The first instrument that enables an international data transfer to be authorised is the existence for an adequacy decision [15] in that country, State, or International Organisation, demonstrating that it guarantees an adequate level of protection, understanding it to be a level equivalent to that granted by the European Union, according to the CJEU *Schrems* [16] Sentence. The status of the adequacy decision, based on the wording of articles 45 and 46 of the GDPR, represents the preferred instrument and the one that best guarantees international transfers, since the wording of article 46 of the GDPR demonstrates that other instruments represent an exception to the existence of an adequacy decision. The minimum content that the British legislation should contain to obtain the adequacy decision is regulated in article 45 of the GDPR [17].

section 3 of Regulation (EU) 2016/679 or article 36, section 3 of Directive (EU) 2016/680.

c. In so far as a decision like those referred to in section 2 has ceased to be applicable, the United Kingdom will guarantee a level of protection for personal data that is essentially equivalent to that established in Union Law regarding the protection of personal data with respect to the processing of the personal data of data subjects referred to in section 1.

[11] Article 134. Facilities offered to auditors in relation to financial provisions

The United Kingdom will notify the Union of the entities it has contracted to audit the application of the financial provisions considered in this part. At the request of the United Kingdom, the Union will provide said contracted entities with any information that may reasonably be requested in relation to the rights and obligations of the United Kingdom by virtue of this part and will give them adequate assistance to enable them to fulfil their mission. By facilitating information and providing assistance by virtue of this article, the Union will act in accordance with applicable Union Law, in particular with Union rules regarding data protection. United Kingdom and Union authorities may agree adequate administrative provisions to facilitate the application of the first and second paragraphs.

[12] Article 72. Confidential processing and restricted use of data and information in the United Kingdom

Without prejudice to the provisions of article 71, as well as Union Law regarding personal data protection, the provisions of the Union Law regarding confidential processing, restricted use, limitation of the conservation period and the obligation to eliminate data and information with respect to data and information obtained by authorities or official bodies from or in the United Kingdom or by contracting authorities as defined in article 4 of Directive 2014/25/EU of the European Parliament and Council (92), from or in the United Kingdom: a) before the end of the transition period; or b) based on this Agreement.

[13] Article 73. The processing of data and information obtained from the United Kingdom

The Union will not process data and information obtained from the United Kingdom before the end of the transition period, or obtained after the end of the transition period based on this Agreement, differently from data and information obtained from a member State simply due to the fact that the United Kingdom has withdrawn from the Union.

[14] Article 74. Information security

1. The provisions of Union Law regarding the protection of classified information from the EU and classified information from Euratom will be applied with respect to classified information obtained by the United Kingdom, either before the end of the transition period, or based on this Agreement, or obtained from the United Kingdom by the Union or a member State either before the end of the transition period, or based on this Agreement.
2. Obligations deriving from Union Law regarding industrial security will be applied to the United Kingdom in cases where the bidding process, contracting or awarding of subsidies relating to a classified contract, a classified subcontract or a classified subsidy agreement, started before the end of the transition period.
3. The United Kingdom will guarantee that cryptographic products that use classified cryptographic algorithms developed under the supervision of a cryptographic certification authority in a member State or the United Kingdom, and evaluated and certified by one of these authorities, and have been certified by the Union until the end of the transition period and are present in the United Kingdom and not transferred to a third country.
4. The requirements, limitations and conditions established in Union certification for cryptographic products will be applied to said products.

[15] An adequacy decision is a decision adopted by the European Commission based on article 45 of the GDPR (for example, the adequacy decision regarding Japan adopted by the Commission on 23rd January 2019). The EU had already adopted other adequacy decisions regarding third countries such as Argentina, New Zealand and Israel, among others). Currently, there is no adequacy decision in force for the United Kingdom.

[16] *Vid.* TJUE Sentence 6th October 2015, Maximillian Schrems / Data Protection Commissioner, C-362/14.

[17] Article 45 Transfers based on an adequacy decision

1. A personal data transfer may be made to a third country or international organisation when the Commission has decided that the third country, a territory or one or more specific sectors of that third country, or the international organisation in question, guarantee an adequate level of protection. Said transfer would not require any specific authorisation.

2. When evaluating the adequacy of the level of protection, the Commission will bear in mind, in particular, the following elements:

a) the Rule of Law, respect for human rights and fundamental freedoms, pertinent legislation, both general and sectoral, including that relating to public safety, defence, national security and criminal law, and access to personal data by public authorities, as well as the application of said legislation, data protection rules, professional rules and security measures, including rules regarding subsequent transfers of personal data to another third country or international organisation, observing the jurisprudence in that country or international organisation, as well

In short, the following should be guaranteed: 1) the content of the rules applicable; and, 2) the means to guarantee their effective application. This content should be completed with the provisions of WP254 of the European Data Protection Committee "References regarding adequacy", which focuses in a more detailed way on the criteria of article 45 of the GDPR. But, observing the new autonomous legislation of the United Kingdom, the United Kingdom should have few obstacles when it comes to pursuing the adequacy decision, but this task will take time and, in the meantime, necessary measures for the circulation of personal data must be taken.

Measures that should be adopted regarding personal data protection after Brexit.

Although the United Kingdom ceases to be a member of the European Union, in accordance with the aforementioned Withdrawal Agreement, it should continue to apply European Union law to all data of data subjects outside the United Kingdom processed before the end of the transition period. This implies that, for the purpose of data export, the United Kingdom's situation is comparable to that of a Member State. To send data to the United Kingdom, it is not necessary to protect oneself with any of the international data transfer instruments provided by the GDPR.

Companies that transfer data to the United Kingdom can continue to do so as they have been doing until now; and it is possible to start new transfers with the same criteria applied to date while the Withdrawal Agreement is in force. Future relations between the European Union and the United Kingdom regarding data protection should be established in the agreements that start to be negotiated after the Withdrawal Agreement comes into force. In the field of data protection, the option that, in principle, seems most likely is that the European Commission could adopt an "adequacy decision" recognising that the United Kingdom offers a level of protection that is essentially equivalent to that provided by the European Union's regulatory framework.

The Withdrawal Agreement itself expressly states that "the European Commission will start, as soon as possible after the withdrawal of the United Kingdom, evaluations regarding said country with the intention of adopting the corresponding decisions, by the end of 2020 at the latest, if the applicable conditions are met". [18] In order to adopt these decisions, the Commission should evaluate the legal system and practice regarding data protection in candidate countries for adaptation, being able to negotiate with them the introduction of regulatory changes or the practical application of regulations that ensure the existence of an adequate level of protection. The decisions should be reviewed regularly in order to verify that the conditions allowing their adoption continue to exist. In the event that a declaration of adequacy is made by means of a Commission decision, data may be sent to the United Kingdom without any type of formal requirement in a similar way in practice to how it would be done for data communications between Member States.

Supervisory system during the transition period.

The GDPR establishes a relatively complex supervisory system based on the system known as "single window". This system consists in, when a data controller or processor has various establishments in the European Union, the supervision of the data processing undertaken is conducted in a cooperative fashion between the supervisory authorities from the countries where establishments exist under the direction and coordination of a "main" supervisory authority which is that of the Member State where the controller or processor's main office is located. The same principle applies when the processing, regardless of whether the controller or processor has various establishments in the Union, significantly affects people in various Member States. According to the terms of the Withdrawal Agreement, the supervisory authority of the United Kingdom can continue to act

as the recognition of the data subjects whose personal data being transferred of effective and enforceable rights and administrative appeals and any effective legal actions;

b) the existence and effective operation of one or several independent supervisory authorities in the third country or those subject to an international organisation, with the responsibility to guarantee and enforce rules regarding the data subjects in the exercise of their rights, and cooperate with the supervisory authorities of the Union and member States, and

c) international commitments assumed by the third country or international organisation in question, or other obligations deriving from legally binding agreements or instruments, as well as their participation in multilateral or regional systems, in particular, in relation to the protection of personal data.

3. The Commission, having evaluated the adequacy of the level of protection, may decide, by means of an execution order, that, in a third country, territory or one or several specific sectors of a third country, or an international organisation, guarantee an adequate level of protection pursuant to the provisions of section 2 of this article. The execution order will establish a regular review mechanism, at least every four years, which takes into account all relevant events in the third country or international organisation. The execution order will specify its sphere of territorial and sectoral application and, where appropriate, will determine the supervisory authority or authorities referred to in section 2, letter b), of this article. The execution order will be adopted according to the examination procedure referred to in article, section 2.

See Execution Decision (EU) 2019/419 of the Commission, of 23rd January 2019, in accordance with Regulation (EU) 2016/679 of the European Parliament and Council, regarding the adequacy of personal data protection on the part of Japan pursuant to the protection of personal data Law («DOUE L» 19th March).

4. The Commission will continuously supervise events in third countries and international organisations that may affect the effective application of decisions adopted according to section 3 of this article and decisions based on article 25, section 6 of Directive 95/46/EC.

5. When the information available, in particular after the review referred to in section 3 of this article, shows that a third country, or an international organisation no longer guarantees an adequate level of protection pursuant to section 2 of this article, the Commission, by means of execution orders, will repeal, modify or suspend, as required and without any retroactive effect, the decision referred to in section 3 of this article. Said execution orders will be adopted according to the examination procedure referred to in article 93, section 2.

For duly justified, overriding, urgent reasons, the Commission will adopt immediately applicable execution orders in accordance with the procedure referred to in article 93, section 3.

6 The Commission will enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision adopted in accordance with section 5.

7. Any decision in accordance with section 5 of this article will be understood without prejudice to personal data transfers to the third country, a territory or one or several specific sectors of that third country, or the international organisation, in question pursuant to articles 46 to 49.

8. The Commission will publish in the Official Journal of the European Union and on its website, a list of third countries, territories and specific sectors in a third country, and international organisations that it has decided that it guarantees, or not, an adequate level of protection.

9. Decisions adopted by the Commission pursuant to article 25, section 6 of Directive 95/46/EC will remain in force until they are modified, substituted or repealed by a Commission decision adopted in accordance with sections 3 to 5 of this article.

[18] *Vid.* https://www.lamoncloa.gob.es/brexit/preparacion2/Paginas/161019.aspx (consultation date: 02/09/2020).

as the "main" authority or an affected authority in procedures involving controllers or processors with an establishment, whether main or not, in the United Kingdom or people in the United Kingdom who are significantly affected by this processing.

The supervisory authority of the United Kingdom should apply the provisions of the GDPR that regulate supervisory procedures and is subject to any decisions that may be adopted by the European Data Protection Committee, the European Union Commission or Court of Justice in cases where the GDPR provides for their intervention. Therefore, the "control model" designed by the GDPR will continue to be applied as it has until now with regard to the supervisory authority of the United Kingdom while the Withdrawal Agreement remains in force.

The sole and substantial difference is that the supervisory authority of the United Kingdom may not take part as a member with voting rights in meetings of the European Data Protection Board (henceforth, the EDPB) engaged in resolving disputes between authorities in the application of these provisions relating to supervision or control.

Impact of Brexit on personal data hosted on networks, IT systems and UK databases.

Another matter of concern is that relating to the hosting of data on networks, IT systems and UK databases and the legal impacts this may entail (one of the main ones being the impact this would have on existing legal and police cooperation within the European Area, which is based on the free circulation of data between the authorities of the Member States and the European Union). This means that, before the end of the Withdrawal Agreement, or the Commission finally not recognising the United Kingdom as a "secure country", the authorities of the European Union and its Member States will cease to have direct access to networks, IT systems and databases of the United Kingdom and, as a result, will need to apply legal frameworks and alternative cooperation mechanisms provided by International Law and all the internal legal systems of the Member State in question.

Although the above does not imply a withdrawal of legal and police cooperation with the United Kingdom, it does translate into fewer guarantees compared to existing policies, protocols and regulations within the territorial sphere of the European Union and the countries that comprise it. For its part, and as logically follows from the above, once the United Kingdom has withdrawn from the European Area, the British authorities will no longer be able to access European Union networks, IT systems and databases. Nonetheless, given the volume of personal data existing on IT systems, whether European Union data in the United Kingdom or data received from the United Kingdom before the withdrawal date, an obligation to delete such data obtained legally by public or private organisations from national or European Union systems, does not exist in all but two cases:

- When the United Kingdom requests deletion due to them holding domain over the data in question; or,
- When the competent authority orders a limitation on processing in accordance with applicable regulations.[19]

Available personal data transfer instruments

In the absence of an adequacy decision after the transition period, the following international personal data transfer instruments will be available to the United Kingdom:

Standard or *ad hoc* Contractual Clauses

The European Union, in its mission to facilitate the international movement of personal data, issued a series of Decisions whereby they approve a clause to be signed between the importer and exporter of personal data whose use enables an international transfer of personal data to be made without the need for an authorisation by the competent supervisory authority. Standard Contractual Clauses are currently divided into two groups, which are:

- When it involves transfers between data controllers; or,
- When it involves transfers between processors.

a. When it involves transfers between data controllers.

In this case, clauses included in Decision 2001/497/EC, of 15th June 2001, regarding standard contractual clauses for personal data transfers to a third country between controllers may be used [20]; and Decision 2004/915/EC, of 27th December 2004, which modifies Decision 2001/497/EC regarding the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third States (consolidated version of 1st April 2005) [21], modified by execution Decision 2016/2297/ EC [22]. The clauses contained in Decision 2001/497/EC provide for a joint and several liability system between the two controllers in the event that the affected party has suffered some kind of harm. By contrast, the set of clauses of Decision 2004/915/EC regulates a liability system based on due diligence [23], whereby the data importer and the data exporter will be accountable to parties affected by their failure to comply with their respective obligations. The exporter will be liable if he/she does not make reasonable efforts to determine whether the importer is capable of fulfilling his/her legal obligations. It provides for greater intervention from the exporter when it comes to resolving claims from affected parties. The control authority will be able to prohibit or suspend transfers more easily if the exporter refuses to take measures against the importer to make him/her fulfil his/her obligations. Both sets of clauses have a rigid composition. Only one of them can be chosen, it not being possible to use clauses from the two models in the same contract, nor modify existing ones.

b. When it involves transfers between processors.

In this event, the clauses included in Decision 2010/87/EU of the Commission, of 5th February 2010, regarding standard contractual clauses for the transfer of personal data to processors established in third countries may be used in accordance with

[19] *Vid.* Medidas de protección de datos y sistemas de información ante un eventual «Brexit» sin acuerdo en (Data protection measures and information systems in the face of a no-deal «Brexit» at): https://www.lealtadis.es/medidas-proteccion-de-datos-y-sistemas-informacion-ante-un-brexit-sin acuerdo/ (consultation date: 02/09/2020).

[20] DOUE L *nº.* 181, of 4th July 2001.

[21] DOUE L *nº.* 385, of 29th December 2004.

[22] DOUE L 344/100, of 17th December 2016.

[23] *Vid.* Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case *(C-362-14).*

Directive 95/46/EC of the European Parliament and the Council, modified by execution Decision 2016/2297/EC [24].

This Decision contains specific clauses for subcontracting a data processor established in a third country to other subprocessors established in third countries. They also add the conditions that the subprocessing should meet to guarantee that the personal data continue to be protected regardless of a subsequent transfer to a data subprocessor. This subprocessing may not exceed the operations stipulated in the contract; whereby it should adapt to the principle of purpose. Even if the subprocessor fails to fulfil his/her obligations, the data importer will remain liable. Like the previous clauses, they are not only enforceable between importers and exporters; they are also enforceable by the affected party when he/she suffers harm deriving from a contractual breach. It is important to emphasise that standard data protection Clauses cannot be modified and should be signed as delivered. Notwithstanding, these contracts may be included in a broader contract and additional clauses may be added provided that they do not, directly or indirectly, contradict the standard data protection Clauses adopted by the European Commission, in line with Recital 109 of the GDPR. If the intention is to modify the content of the clauses, they will be deemed to be a*d hoc* contracts. These contracts involve contractual clauses that are not recognised by the Commission with respect to the content of the clause, whereby guaranteeing the content falls on the control authority. Before making any transfer based on *ad hoc* clauses, the national control authority must authorise these adapted contractual clauses subject to a prior ruling by the EDPB [25].

Binding Corporate Rules.

When it comes to international data transfers between companies from the same group, the GDPR provides for a "tailored" system for those entities, known as Binding Corporate Rules (henceforth, BCR). Recital 110 of the GDPR grants the possibility for a business group to be able to invoke authorised BCR's to make international data transfers to other group entities located in third countries provided that such rules include the necessary guarantees and will not replace mandatory data protection legislation under any circumstances [26].

Currently, article 4.20) of the GDPR defines them as "personal data protection policies assumed by a data controller or processor established in the territory of a member State for transfers or a set of personal data transfers to a data controller or processor in one or more third countries, within a business group or a union of companies engaged in a joint economic activity". In short, they are internal rules adopted by a multinational group with respect to international personal data transfers within the same business group to entities located in countries that do not offer an adequate level of protection. They are only intended for business groups.

International data transfers from the United Kingdom to European Union member states.

When it comes to international transfers from the United Kingdom to the European Union, this will depend on the legal system remaining between the United Kingdom and the European Union. If, in the end, the agreement is approved, European Union Law will continue to be applied, whereby nothing will change in this sense, at least during the transition period.

Otherwise, and given that the United Kingdom ceases to obey European regulations, responsibility for determining the legality of international personal data transfers will fall on its internal Law. In this event, we must resort to the system created by the GDPR and the *Data Protection Act 2018*. In this sense, by adopting the GDPR as an autonomous regulation, they assume the same international personal data transfer instruments; such that the United Kingdom will:

- Recognise EEA States as secure countries;
- Recognise countries that have been declared secure countries by the European Union;
- Assume European Commission models for Standard Contractual Clauses; and
- Maintain authorisations provided for BCR's.

To facilitate this transition, the *Information Commissioner's Officer* has issued a series of templates for making international transfers by means of Standard Contractual Clauses.

Extraterritorial application of the GDPR and international private relations.

Once Brexit finally materialises and the transition period ends, the following will apply to controllers and processors who process the personal data of people in the European Union: a) rules regarding the extraterritorial application of the GDPR in accordance with article 3 of the GDPR, according to Directives 3/2018 regarding the territorial application of the GDPR, of the European Data Protection Board; and, b) the rules of private international Law when it comes to dealing with both contractual and non-contractual claims regarding data protection.

1. Extraterritorial application of the GDPR in activities to establish a controller or processor in the European Union.

a. Concept of establishment in the European Union.

Article 3.1 of the GDPR stipulates that European legislation will be applied when the data processing is undertaken in the context of an establishment of a controller or processor in the European Union regardless of whether the processing takes place in the Union or not. Thus, European legislation will apply to any action undertaken on the personal data of any individual within the sphere of the Union. It is due to this assumption of subordination that all British companies that have branches, or subsidiary entities, will be subject to this legislation. The issue most discussed by the CJEU has been the definition of "establishment". Recital 22 of the GDPR states that "an establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not a determining factor in that respect [27].

[24] DOUE L 344/100, of 17th December 2016.

[25] *Vid.* ORTEGA GIMÉNEZ, Alfonso and GONZALO DOMENECH, Juan José, "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro" ? (Brexit and personal data protection: will the United Kingdom cease to be a "safe country"?), in *Revista Aranzadi Unión Europea*, *núm.* 11/2019, Editorial Aranzadi, 2019, pp. 1-23.

[26] *Vid.* THOMAS, H. *et al*., *Legal Aspects of Digital Preservation*, Cheltenham, Edward Elgar Publishing, 2013, p. 86.

[27] *Vid.* TJUE *Weltimmo* Sentence (Issue C-230/14) of 1st October 2015. ECLI: EU: C: 2015:639.

The concept of "establishment" extends to any real and effective activity, however slight, exercised through a stable installation. This flexible concept of establishment is used to guarantee the right to data protection as stated in Recital 23 of the GDPR. Once the one of article 4. 16) of the GDPR was described, its definition considered the concept of "main establishment". The inclusion of said definition clarifies and delimits highly relevant issues such as the specification of the main establishment of a data controller or processor with various establishments in the Union by means of rules established by the principle of speciality and hierarchy. Thus, in the case of a controller with several establishments, as a general rule, the main establishment will be deemed to be the one from where the central administration is undertaken in the Union. But, as a special rule, if decisions about the purposes and means of the processing are taken in another establishment, and it has the power to implement them, the latter will be deemed to be the main one. Regarding the case of a data processor with various establishments, the main establishment will be deemed to be the one from where the central administration is undertaken in the Union. If this is lacking, as a supplementary rule, it will be the processor's establishment in the European Union where the main processing activities, in the context of the activities of a processor's establishment, are undertaken [28].

b. The relationship between the establishment and data processing activities undertaken.

As stated above, and as ordered in repeated CJEU Sentences [29], such processing should be undertaken "in the context of the establishment's activities". To explain such a concept, we should refer to the aforementioned Directives 3/2018.

To clarify this relationship, the European Data Protection Board reminds us that the jurisprudence of the CJEU Sentence in the *Google Spain* case requires confirmation that the activities of a local establishment and data processing activities may be inextricably linked, even if that establishment is not really playing any role in the data processing itself. If the data processing is undertaken by establishments not established in the Union, and the establishment in the Union does not intervene in said processing, the activities undertaken by that establishment may, alternatively, grant the protection offered by European legislation, provided that an "inextricable link" exists between the activities of the establishment in the Union and the data processing, regardless of whether the processing is undertaken in the Union. Clearly understanding the fact of subordination, geographical location no longer matters, rather the means-end relationship between the personal data processing and the activity undertaken; not even those whose personal data are being processed are differentiated provided that they are in the European Union. Gone is the interpretation resulting from a defective wording of article 3 of the GDPR, corrected by the Error Correction of 23rd May 2018, which limited the application to the personal data of people residing in the European Union [30].

c. Location criterion in responsible relations between controllers and processors.

Based on the primacy of the relationship of the activity with the data processing regarding the geographical location of the processing, the location criterion is used when it comes to determining the application of the obligations to data controllers and processors. We should affirm that, although both subjects are characterised by processing personal data, they do not have the same obligation regimes. The obligation regime for a data controller is governed solely by law; by contrast, the regime for a data processor will vary if it is located in the European Union or in a third State. If the processor is located in the European Union, the obligations of the GDPR will not only apply, but also the contractual provisions of 28 of the GDPR, in particular, regarding the collaboration regime between the processor and controller in the fulfilment of the latter's obligations. By contrast, if the processor is located outside the European Union, the GDPR may not be applied, as it is not deemed to be the controller's establishment, nor are the data of European citizens being processed, whereby the application of the GDPR is determined by the contractual obligations established in the contract. In addition to this, in the event that a controller in the European Union resorts to a British processor, Standard Contractual Clauses should be used with additional guarantees for making an international transfer.

2. Processing activities relating to the supply of goods or services regardless of whether they are required to pay.

a. Concept of a data subject "who is in the European Union".

The criterion of article 3.2 facilitates the subjugation to European legislation to those not established in the Union and process the data of individuals who are in this territory in circumstances that can be seen to require them to be applied [31]. This article was modified to clarify the wording and scope of application as outlined above, since the version in other languages, such as Spanish, required that data subjects "reside" in the European Union, such that the scope of application was limited to a more adequate one, avoiding an abusive exceedance in the scope of application [32].

[28] *Vid.* ORTEGA GIMÉNEZ, Alfonso and GONZALO DOMENECH, Juan José, "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro"?, en *Revista Aranzadi Unión Europea*, *núm.* 11/2019, Editorial Aranzadi, 2019, pp. 1-23.

[29] *Vid.* STJUE *Google Spain*, C-131/12, ECLI:EU:C:2013:424 (pár. 52); *Weltimmo*, C-230/14 ECLI:EU:C:2015:639 (pár. 35), y *Amazon EU Sàrl*, C-362/14 ECLI:EU:C:2015:650 (p. 78).

[30] *Vid.* ORTEGA GIMÉNEZ, Alfonso y GONZALO DOMENECH, Juan José, "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro" ?, (Brexit and personal data protection: will the United Kingdom cease to be a "safe country"?), in *Revista Aranzadi Unión Europea*, *núm.* 11/2019, Editorial Aranzadi, 2019, pp. 1-23.

[31] *Vid.* DE MIGUEL ASENSIO, P. A.: "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea" (Competence and applicable Law in the General Data Protection Regulation of the European Union), in *Revista Española de Derecho Internacional*, 2015, *núm.* 1º, vol. 69, 2017, p. 14.

[32] *Vid.* BRKAN, M., "Data protection and conflict-of-laws: a challenging relationship", in *European Data Protection Law Review*, 2016, *núm*. 3o, vol. 2, p. 337; SVANTESSON, D. J., *Extraterritoriality in Data Privacy Law*, Ex tuto Publishing, Copenhague, 2013, p. 107. GONZALO DOMENECH, J. J., "Algunas cuestiones relevantes de Derecho internacional privado en el Reglamento General de Protección de Datos" (Some relevant questions from private international Law in the General Data Protection Regulation), in *Revista Boliviana de Derecho*, nº 26, 2018, p. 413.

b. Offer of goods and services to data subjects in the European Union.

The GDPR requires a series of conditions to be met: a) The effective processing of personal data; and b) The controller's activities be directed at data subjects in the European Union.

We should start from the description made in Recital 23 of the GDPR, which determines whether the controller or processor is offering good or services to affected parties who are in the Union, we must determine whether it is evident that the controller or processor plans to offer services to affected parties in one or several member States of the Union (*targeting-based analysis*) [33]. The Recital does not deem website accessibility, the use of a common third language or contact details to be indications that services and products are being offered in the Union, as ruled in the CJEU *Wertimmo* Sentence. It does deem, by contrast, language use, currency or the mention of clients or users that reside in the Union to be indications that the controller or processor is aiming his/her offer to Union territory, with a clear focus on the doctrine established in the CJEU *Pammer and Hotel Alpenhor* Sentence [34], consolidated in the CJEU *Mühlleitner* [35], and *Emrek* [36-37] Sentences and endorsed by the EDPB.

Jurisprudence compels the existence of an activity directed by means of certain indications to be evaluated, such as the offer of such services or products in member States of the European Union, or advertising in different media that facilitates awareness among consumers. The EDPB, in accordance with jurisprudential doctrine offers a non-exhaustive list of indications, whereby the following are deemed to be as such [38]:

- The EU, or at least the member State, is designated by name in relation to the good or service offered;
- The data controller or processor pays a search engine operator for an Internet referencing service for the purpose of facilitating access to his/her website for Union consumers; or, the data controller or processor has launched commercialisation campaigns and advertising aimed at the public of an EU country.
- The international nature of the activity in question, such as certain touristic activities;
- The mention of addresses or specific telephone numbers that can be accessed from an EU country;
- The use of a different top-level domain name from the third country where the controller or processor is established, for example, ".de", or the use of neutral top-level domain names, such as ".eu";
- Description of travel instructions from one or more EU member States to the place where the service is provided;
- The mention of an international clientele made up of clients domiciled in various EU member States, in particular, by submitting accounts created by said clients;
- The use of a language or currency that is different to that generally used in the trader's country, especially a language or currency of one or more EU member States; and/or
- The data controller offers delivery of goods in EU member States.

This should be restricted to processing activity determined by applying the regulations, not to the rest of his/her activities that have no relation to the offer of goods and services, since a contrary application would exceed the object that it seeks to protect.

Future perspectives: personal data protection and the New Association Agreement EU-United Kingdom.

On 18th March 2020, the European Commission sent the United Kingdom a draft legal Agreement that considers the future Association between the European Union and the United Kingdom [39]. The draft captures the directives of negotiations approved by the General Affairs Council on 25th February 2020, in accordance with the political declaration agreed between the EU and the United Kingdom in October 2019.

The Commission proposes clarifying a series of areas that go beyond what the EU usually engages in with third countries, in so far as it is proposing provision for cooperation in foreign affairs or security and defence. Cooperation in these spheres is clearly mutually beneficial to both citizens of the EU and the United Kingdom. In this sense, the EU is really offering the United Kingdom cooperation of an unprecedented nature [40].

In this context, Title VII ("ELECTRONIC COMMERCE") of the aforementioned draft Agreement mentions "data flows and personal data protection", in its second Chapter (in particular, in articles 6 and 7), establishing the following as main guidelines: a) the recognition of personal data protection and privacy as a fundamental right (article 7.1 of the draft Agreement); b) the commitment of the EU and the United Kingdom to guarantee cross-border data flows to facilitate commercial relations (article 6 of the draft Agreement; and, c) the adoption and maintenance of safeguards deemed to be adequate for guaranteeing privacy and the protection of personal data by both the EU and the United Kingdom, including the adoption and application of rules for the cross-border transfer of personal data (article 7.2 of the draft Agreement).

This being the case, as we can see, the United Kingdom leaving the European Union is going to have important consequences with regard to personal data protection. And, as we have analysed, it will become a "third country" for the purposes of applying the GDPR, whereby the tools provided for international data transfers need to be borne in mind, with all the difficulties and costs that this generates for companies.

[33] *Vid.* GEIST, M., "Is There a There? Toward Greater Certainty for Internet Jurisdiction", 2001, in *Berkeley Technology Law Journal, núm.* 3º, vol. 16, pp. 1345-1406.

[34] *Vid.* TJUE Sentence of 7th December 2010, *Pammer and Hotel Alpenhof*, C-585/08, ECLI: EU: C: 2010: 740.

[35] *Vid.* TJUE Sentence of 6th September 2012, *Daniela Mühlleitner*, C-190/11.

[36] *Vid.* TJUE Sentence of 17th October 2013, *Emrek*, C-218/12, ECLI: EU: C: 2013:494.

[37] *Vid.* The case dealt with in the CJEU Sentence cited does not deal with data protection but disputes in commercial matters.

[38] The doctrine established by the CJEU derives from the one established by the US *Supreme Court, Calder v. Jones* (465 U.S. 783 (1984)), whereby courts are allowed whether a determined target market exists through the use of elements such as the language used, currency, or nationality. Although some sectors understand that this doctrine can be blamed for its strong subjective component. JIMÉNEZ-BENÍTEZ, W. G., "Rules for Offline and Online in Determining Internet Jurisdiction", *Revista Colombiana de Derecho Internacional*, 16, 2015, p. 30.

[39] Text available (English version): https://ec.europa.eu/info/publications/draft-text-agreement-new-partnership-united-kingdom

[40] *Vid.* https://fernandezrozas.com/2020/03/23/brexit-proyecto-de-acuerdo-de-nueva-asociacion-ue-reino-unido-de-18-de-marzo-de-2020.

Despite the recent materialisation of Brexit, this does not mean full exemption from compliance with the GDPR since, in the event of a British entity processing the personal data of citizens who are in the European Union, whether within said draft framework Agreement, or through extraterritorial application of the GDPR, it must meet its RDPR obligations.

And everything points to the United Kingdom will be deemed to be a "secure country" since it has already demonstrated that, despite leaving the European Union, it will do everything possible to maintain a "high level of protection" with respect to data protection in the terms required by the GDPR (the approval of the *Data Protection Act 2018* accredits this and, proof of this is its adaptation to the GDPR) and the EU "recognises" this in its draft legal Agreement that contemplates its future Association with the United Kingdom.

References

1. Brkan M. "Data protection and conflict-of-laws: a challenging relationship", en European Data Protection Law Review. 2016; 3(2):337;
2. Svantesson DJ. Extraterritoriality in Data Privacy Law, Ex tuto Publishing, Copenhague, 2013.
3. Corral Sastre A. "Las transferencias de datos personales al Reino Unido en la era postbrexit", en Diario la Ley, Especial Revista de Derecho Digital e Innovación, 2019, (3).
4. De Hert P, Papa Konstantinou y V. The rich contribution to the field of EU data protection: Let's not go for third country status after Brexit, en Computer Law & Security Review, 2017, (33).
5. De Miguel Asensio PA. "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", en Revista Española de Derecho Internacional núm, 2015, 69(1).
6. Geist M. "Is There a There? Toward Greater Certainty for Internet Jurisdiction", 2001, en Berkeley Technology Law Journal, núm, 2001, 16(3).
7. Gonzalo domenech JJ. "Algunas cuestiones relevantes de Derecho internacional privado en el Reglamento General de Protección de Datos", en Revista Boliviana de Derecho, 2018, (26).
8. Jiménez-Benítez WG. "Rules for Offline and Online in Determining Internet Jurisdiction", Revista Colombiana de Derecho Internacional, 2015, 16.
9. Ortega Giménez Alfonso. "Brexit, relaciones privadas internacionales y protección de datos de carácter personal: ¿y ahora qué?... ¿dejará de ser el Reino Unido un "país seguro"?, en Revista Diario LA LEY Unión Europea, núm. 80, marzo 2020, Editorial Aranzadi, 2020.
10. Ortega Giménez, Alfonso y Gonzalo Domenech, Juan José. "Brexit y protección de datos de carácter personal: ¿dejará de ser el Reino Unido un "país seguro"?, en Revista Aranzadi Unión Europea, núm. 11/2019, Editorial Aranzadi, 2019.
11. Thomas H. y otros, Legal Aspects of Digital Preservation, Cheltenham, Edward Elgar Publishing, 2013.