BREXIT

Personal Data:
Safeguards for Brexit

If your company has a supplier, parent company, subsidiary or partner located in the United Kingdom, it most probably means that you are transferring personal data to the UK. It is therefore highly advisable to know **what can be done** in the event that **Brexit** ultimately goes ahead, in order to be able to continue transferring that information and benefitting from those business relationships **without breaching data protection regulations** or being exposed to the resulting severe penalties.

Once the United Kingdom has left the European Union, communications of personal data to the UK will be considered **international data transfers**, since it will become a third country (non-EU and non-EEA).

The General Data Protection Regulation (GDPR) is the world's most stringent legislation in the area of privacy. It therefore follows that if the data is sent to a country outside the European Economic Area (EEA), the level of security and safeguards will be lower. Thus, the general rule is that **such data flows shall not be permitted unless the following criteria are fulfilled**:

- **The country of destination for the data has an "Adequacy Decision"**: The European Commission, having studied the country's privacy legislation, considers that it provides sufficient guarantees in keeping with European standards, as was recently the case with Japan in the ruling adopted on 24 January. However, while the United Kingdom has adapted its national legislation in line with the European data protection regulation (GDPR), the European Data Protection Board or EDPB (which replaced the Article 29 Working Party) has already pointed out that at the present time, the UK does not have an adequacy decision, and the fact is that the process of adopting the decision could take up precious time during which data flows to the United Kingdom cannot be stopped.

- **Appropriate safeguards have been adopted**: even if the destination country does not have an adequacy decision, the transfer of data can be enabled if appropriate safeguards are provided, the most important of which are the following:

  - **Standard clauses**: contractual provisions that oblige the recipient of the data to adopt measures and safeguards that provide for a level of protection comparable to the European level.
  - **Binding corporate rules**: better known as BCR, they are a set of legally binding policies or codes of conduct developed and implemented by a group of enterprises in order to provide sufficient guarantees for the secure transfer of data within the group. This mechanism is exclusively for groups of enterprises, and the rules must be submitted to the pertinent supervisory authority for review and, where appropriate, approval.

- **Codes of conduct and certification mechanisms**: these mechanisms are a new feature introduced by the GDPR. The codes of conduct are self-regulatory sectoral rules. The approach is similar to that of BCR, but applied to a business sector rather than to a group of enterprises. Moreover, the GDPR provides for the possibility to create certification mechanisms in the area of data protection (such as seals or marks) as a means of demonstrating compliance with the applicable legislation. The EDPB is currently working on a series of directives to harmonise these conditions.

- **One of the legally established derogations applies**: the GDPR does leave some room for manoeuvre, establishing that even if the destination of the international data transfer is not deemed secure and adequate safeguards are not provided for data communication, it may be permitted in the event that it comes under any of the established exceptions. The EDPB has already cautioned that, since these are exceptions, they must be interpreted restrictively, and only be used occasionally to ensure that the exception does not become the rule.

Thus, even if the United Kingdom did not manage to conclude an agreement before its departure from the European Union, or if the agreement did not contain any provisions on data protection, **this would not necessarily imply cutting off the flow of personal data from the EU**, although the flow of data would depend on the decision that the European Union decides to adopt, and on the preparedness or quick response of companies in the rest of Europe that have business relationships with the United Kingdom.

Please do not hesitate to write to your usual contact at ELZABURU or to brexit@elzaburu.es in case you need further clarification on these aspects or any other related to the Brexit

Calle Miguel Ángel, 21
28010 Madrid, España
+34 917 009 400
brexit@elzaburu.es
www.elzaburu.es/en/brexit