ELZABURU

Marzo 2019

BREXIT

Datos personales:
Salvaguardas para el Brexit

Si su empresa tiene algún proveedor, matriz, filial, partner o colaborador establecido en Reino Unido, es muy probable que esté transfiriendo datos personales a dicho país. En ese caso, es sumamente conveniente **saber qué puede hacerse**, si finalmente llega el **Brexit**, para poder seguir transfiriendo esa información y beneficiándose de esas relaciones **sin incumplir la normativa** sobre protección de datos ni exponerse a duras sanciones por ello.

Y es que, una vez se haya consumado la desvinculación de Reino Unido, las comunicaciones de datos personales a dicho país serán consideradas como **Transferencias Internacionales de Datos (TID)**, al pasar a ser un país tercero de la UE y del EEE.

El Reglamento General de Protección de Datos (RGPD) es la normativa más estricta en materia de privacidad a nivel mundial. De ello se deriva que, en caso de que los datos se envíen a un país fuera del Espacio Económico Europeo (EEE), el nivel de seguridad y garantías disminuyen. Así, la regla general es que **no se permiten esos flujos de datos salvo que se cumpla** alguno de los siguientes supuestos:

- **Que el país de destino de los datos cuente con una Decisión de Adecuación**: la Comisión Europea, tras estudiar la normativa de privacidad del país, considera que reviste las garantías suficientes para estar acorde al nivel europeo, como ha sido el reciente caso de Japón el pasado 24 de enero. Sin embargo, aunque el Reino Unido ha adaptado su legislación nacional al Reglamento europeo de Protección de Datos (el RGPD), el Comité Europeo de Protección de Datos o CEPD (el antiguo Grupo de Trabajo del Artículo 29) ya apunta que, a día de hoy, no cuenta con tal decisión de adecuación y lo cierto es que su tramitación puede llevar un tiempo precioso durante el que no se pueden paralizar los flujos de datos al Reino Unido.

- **Que se hayan adoptado garantías adecuadas**: aun sin contar el país de destino con una decisión de adecuación, se puede habilitar la transferencia de datos si se cuenta con alguna de las garantías que la avalan, de las cuales las más importantes son:

  - **Cláusulas tipo**: previsiones contractuales que obligan al receptor de los datos a adoptar medidas y garantías que permiten un nivel de protección equiparable al europeo.

  - **Normas corporativas vinculantes**: más conocidas por sus siglas en inglés, las BCR (*Binding Corporate Rules*), consisten en un conjunto de normas políticas o códigos de conducta jurídicamente vinculantes que un grupo de empresas diseña e implanta, con la finalidad de ofrecer las garantías suficientes para que las transferencias de datos intra grupo resulten seguras. Es un mecanismo exclusivo para los grupos empresariales, y deben presentarse a la Autoridad de Control pertinente para su revisión y, en su caso aceptación.

- **Códigos de conducta y mecanismos de certificación**: estos mecanismos son una novedad introducida por el RGPD. Los códigos de conducta consisten en normas sectoriales de autorregulación, el planteamiento es similar al de las BCR pero en lugar de a un grupo industrial, aplicado a un sector empresarial. De otra, el RGPD establece la posibilidad de la creación de mecanismos de certificación en materia de protección de datos (tales como sellos o marcas) a fin de demostrar el cumplimiento de la normativa aplicable. El CEPD está actualmente trabajando en una serie de directrices para armonizar estas condiciones.

- **Que resulte aplicable alguna de las excepciones tasadas**: el RGPD deja algo de margen, estableciendo que, aun cuando la TID esté dirigida a un destino que no se considere seguro, ni tampoco se haya blindado la comunicación con garantías adecuadas, se podrá llevar a cabo en caso de que se pueda amparar en algunas de las situaciones excepcionales que contempla. El CEPD ya advierte que, al tratarse de excepciones deben ser interpretadas de una manera estricta, debiendo acudir a las mismas sólo de manera ocasional y no como regla general.

De esta suerte, aun cuando el Reino Unido no lograra alcanzar un acuerdo antes de su marcha definitiva, o si dicho acuerdo no contempla previsiones en materia de protección de datos, **no conllevaría necesariamente el aislamiento de flujos de datos personales de la UE**, si bien su fluidez dependerá de la decisión que le merezca a la Unión Europea, y de la anticipación o rápida respuesta por parte de las empresas del resto de Europa que tengan relación con el Reino Unido.

Actualización enero 2020:

El pasado 31 de diciembre de 2020, se alcanzó el "Acuerdo de Comercio y Cooperación entre la Unión Europea y la Comunidad Europea de la Energía Atómica, por una parte, y el Reino Unido de Gran Bretaña e Irlanda del Norte, por otra".

Este acuerdo tiene un carácter exhaustivo y, entre otros muchos aspectos, trata la regulación de los flujos de datos entre la Unión Europea y el Reino Unido. Así, en el artículo FINPROV.10ª de este Acuerdo se establece que la transmisión de datos personales de la UE al Reino Unido no se considerará Transferencia Internacional de Datos en tanto no transcurran cuatro meses (más dos de prórroga) desde la fecha del Acuerdo.

Las partes en el Acuerdo prevén que, antes de este plazo, se habrán realizado todas las acciones necesarias para que el Reino Unido cuente con una Decisión de Adecuación que ampare los flujos de datos personales internacionales de la UE a aquel.

Por favor, no duden en escribir a su contacto habitual en ELZABURU o al correo brexit@elzaburu.es en el caso de que necesiten más aclaraciones sobre estos aspectos o cualquier otro relacionado con el Brexit.

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