CincoDías
Jueves 17 de diciembre de 2020

LEGAL

Wolters Kluwer

Privacidad

Guía legal para que las empresas transfieran datos a EE UU de forma segura

Existe inseguridad jurídica desde la anulación del 'Privacy Shield'

Debe haber proactividad en las vías para minimizar riesgos, dicen los analistas

IRENE CORTÉS
MADRID

En julio de este año, el Tribunal de Justicia de la Unión Europea (TJUE) dictó una sentencia en la que invalidaba el *Privacy Shield* (en español, escudo de privacidad), el acuerdo entre Estados Unidos y la UE para regular las transferencias de datos entre ambos territorios. Los magistrados comunitarios consideraron que el sistema no cumplía con las garantías que exige el Reglamento General de Protección de Datos (RGPD).

El fallo dibujó un escenario complicado para muchas empresas españolas. "Al principio hubo mucha preocupación ya que un gran número de compañías tienen sus servidores en entidades estadounidenses", recuerda María Zarzalejos, asociada en el área de privacidad de Andersen. No es para menos: las infracciones en materia de protección de datos conllevan multas de hasta 20 millones de euros o el 4% de la facturación global de la compañía en los casos más graves.

¿Qué deben hacer las organizaciones para poder convertir en legítimas las transferencias de datos? "Para empezar, deben ponerse en contacto con los servidores para anular el traslado de información a Estados Unidos", aconseja. En este sentido, poco después de publicarse la sentencia, gigantes tecnológicos como Amazon, Google o Apple anunciaron que iban a trasladar la información que viene de compañías europeas a sus servidores ubicados en el continente.

Cláusulas tipo

Otra vía legal son las cláusulas contractuales tipo, o las SCC por sus siglas en inglés (*standard contractual clauses*). Este instrumento legal permite realizar transferencias internacionales con garantías, suscribiendo un contrato entre el exportador e importador de los datos por el que el último se compromete a tratar la información respetando la normativa europea.

En su sentencia, el tribunal europeo confirmó la validez de estas cláusulas, si bien matizó que el responsable debe hacer una evaluación previa del contenido de las SCC para garantizar que se mantiene un nivel de protección equivalente al fijado en el RGPD. En este sentido, el Comité Europeo de Protección de Datos (CEPD) ha emitido varios documentos en los que concreta que el análisis debe abarcar desde las circunstancias específicas de la transferencia hasta el régimen jurídico aplicable en el país importador.

Es decir, que las entidades deben valorar si la legislación o la práctica del país receptor de la información podría suponer un obstáculo para el cumplimiento de las obligaciones en materia de privacidad. De ser así, el organismo europeo aconseja adoptar medidas de salvaguarda adicionales.

Actitud proactiva

Por su parte, Isabel Martínez, directora del área de privacidad de Andersen, destaca que las empresas deben cumplir con "el principio de *accountability*" (o responsabilidad). Es decir, que deben mostrar una actitud proactiva e implementar las medidas adicionales que crean convenientes para cumplir con el reglamento europeo. Asimismo, deberán monitorizar las decisiones adoptadas "para asegurarse de que las transferencias internacionales de datos se están llevando a cabo correctamente", asevera la jurista.

Empresas como Amazon o Google han trasladado los datos a servidores europeos

Las entidades deben analizar las SCC para verificar que respetan la privacidad

Si bien los organismos europeos han arrojado un poco de luz con sus recomendaciones, lo cierto es que las empresas no lo tienen nada fácil. Al fin y al cabo, la revisión de las SCC es un trabajo muy exhaustivo que requiere un esfuerzo extra por parte de las entidades.

En este sentido, Zarzalejos es optimista y descarta que las autoridades en protección de datos vayan a sancionar a las empresas que sigan transfiriendo datos con EE UU, "siempre que muestren una actitud proactiva y hayan realizado el análisis de las cláusulas contractuales tipo".

En todo caso, la abogada recomienda evitar suscribir nuevos contratos o ejecutar operaciones que supongan la trasferencia datos personales a Estados Unidos, optando en su lugar por plataformas radicadas en países europeos "donde también sea de aplicación el RGPD".

Transferencias de datos con el Reino Unido

► Brexit. La salida del Reino Unido de la Unión Europea está generando muchas dudas por parte de las compañías. Así lo confirma María Zarzalejos, abogada en Andersen, que aclara que la materialización del Brexit convertirá las transferencias de datos con el país británico en intercambios internacionales, lo que exige a las empresas implementar medidas adicionales de protección. No obstante, la letrada considera que este escenario no será tan problemático como el estadounidense. En primer lugar, "porque todavía existe la posibilidad de llegar a un acuerdo". Y segundo, porque la cultura de privacidad en el Reino Unido es más parecida a la europea, por lo que es probable que su legislación se ajuste a los mínimos fijados en el RGPD. De hecho, el Gobierno británico ya anunció que absorberá el reglamento en su ordenamiento.

► Revisión. De todas formas, y sin perjuicio de que haya acuerdo, Zarzalejos aconseja a las compañías que realicen intercambio de información personal con el Reino Unido que revisen los flujos de datos que pudieran verse afectados y adopten las medidas necesarias, entre ellas la suscripción (o revisión en el caso de que ya existieran) de las cláusulas contractuales tipo.