Protección de los datos personales transferidos fuera de la UE (I y II)

Florina Pop, Profesora Titular

EIPA Maastricht

Financiado por la Unión Europea

Transferencia de datos personales

- «**Cuando los datos personales viajan, la protección de los mismos también debería viajar con ellos...**» (Comisaria Jouroba, Comisaria Europea de Justicia, Consumidores e Igualdad de Género)
- **El Capítulo V del RGPD no define la *transferencia***

El CEPD ha identificado tres criterios para que un tratamiento de datos se considere una transferencia

1) El responsable o encargado del tratamiento está cubierto por el RGPD para dicho tratamiento

2) Al transmitir los datos personales tratados, dicho responsable o encargado («exportador») comunica dichos datos o los pone a disposición de otro responsable, corresponsable o encargado

3) El importador se encuentra en un tercer país o es una organización internacional, independientemente de si se le aplica el RGPD en el contexto de este tratamiento, a la luz del artículo 3 del RGPD

Transferencia de datos personales

La transferencia de datos personales a un país no comunitario / que no forme parte del EEE únicamente puede producirse si:

- El destino ha sido objeto de una decisión de adecuación (Artículo 45 RGPD)
- A falta de una decisión de adecuación, si la transferencia hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas (Artículo 46 RGPD)

Y... POSTERIORMENTE INCLUYE ANGUNAS CONDICIONES ESTRICTAS PARA:

Derogaciones (Artículo 49 GDPR)

Estructura del RGPD

- Los responsables pueden transferir los datos personales, en orden descendiente, empezando por una **decisión de adecuación basada en el RGPD (I).**
- A falta de una decisión de adecuación, las transferencias deben ofrecer las **garantías adecuadas (II)**.
- De no existir garantías adecuadas, serán de aplicación **derogaciones para situaciones específicas** (III). Se trata de una opción de último recurso para circunstancias excepcionales con la que hay que ser cautelosos.
- **Si (I), no hace falta pasar al (II).**

Requisitos para una transferencia lícita

Una transferencia es una operación de tratamiento de datos (Artículo 4, apartado 2) y únicamente será lícita si cumple con todos los requisitos de protección de datos personales, incluyendo:

Valorar la adecuación

Decisiones de adecuación

Las decisiones de adecuación son decisiones adoptadas por la Comisión sobre la adecuación de un país u organización para ser el destinatario de la transferencia de datos personales. Normalmente se debe a que el país cumple con una serie de criterios legales.

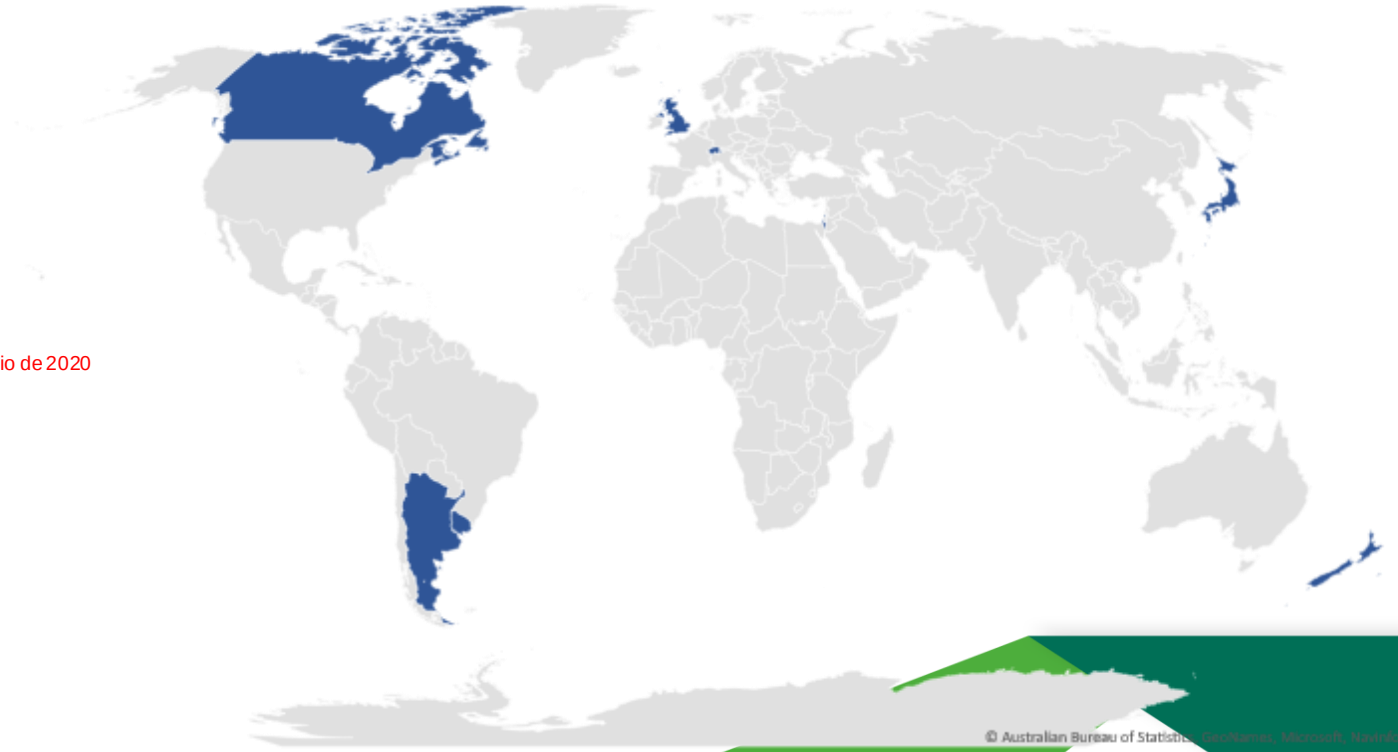
Los criterios de adecuación requieren que el país al menos disponga de:

- **Estado de derecho**
- **Acceso a la justicia**
- Respeto de los **derechos humanos y las libertades fundamentales**
- Legislación relevante, tanto general como sectorial, sobre: **seguridad pública, defensa, seguridad nacional, orden público y derecho penal**
- Existencia de una **autoridad de control independiente que garantice el cumplimiento**
- **Adhesión a compromisos internacionales vinculantes** del tercer país, sobre todo con respecto a la protección de datos personales

¿Qué sucede en el resto del mundo?

Países que la Comisión Europea considera que proporcionan un nivel adecuado de protección

Suiza 26 de julio de 2000
Canadá 20 de diciembre de 2001 (organizaciones comerciales)
Argentina 30 de junio de 2003
Guernsey 21de noviembre de 2003
Isla de Man 28 de abril de 2004
Jersey 8 de mayo de 2008
Islas Feroe 5 de marzo de 2010
Andorra 19 de octubre de 2010
Israel 31 de enero de 2011
Uruguay 21 de agosto de 2012
Nueva Zelanda 19 de diciembre de 2012
Japón 23 de enero de 2019
~~**Estados Unidos: Escudo de la privacidad**~~ invalidado 16 de julio de 2020
Reino Unido 28 de junio de 2021
Reciente
Corea del Sur 17 de diciembre de 2021



Dos categorías de garantías adecuadas

1.
   - Garantías que NO requieren una autorización específica de la APD (lista cerrada)
2.
   - Garantías que requieren una autorización de la APD (lista abierta)

Salvaguardas adecuadas

Salvaguardas (II)

El Reglamento proporciona un conjunto de garantías, algunas de las cuales requieren la aprobación específica de la autoridad de control antes de considerar que cumplen con el Reglamento:

- Instrumento legalmente vinculante y ejecutable entre autoridades u organismos públicos
- Normas corporativas vinculantes
- Cláusulas estándar de protección de datos adoptadas por la Comisión.
- Cláusulas estándar de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
- Código de conducta con compromisos vinculantes y ejecutables del responsable o encargado en el tercer país para aplicar las garantías adecuadas y proteger los derechos de los interesados
- Mecanismo de certificación con compromisos vinculantes y ejecutables del responsable o encargado en el tercer país para aplicar las garantías adecuadas y proteger los derechos de los interesados.
- Cláusulas contractuales entre el responsable/encargado y el responsable/encargado/destinatario en el país tercero o la organización internacional.
- Los acuerdos administrativos entre las autoridades organismos públicos incluyendo exposiciones en las que se estipulan los derechos efectivos de los interesados

Garantías adecuadas

Normas corporativas vinculantes

Las *normas corporativas vinculantes* están definidas en el RGPD:

- Las *normas corporativas vinculantes* son las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Derogaciones

1.Con el consentimiento del interesado, tras haberle informado de los riesgos, sobre todo de los resultantes de la ausencia de garantías y de la falta de una decisión de adecuación.

2.Si la transferencia es necesaria para honrar un contrato entre el interesado y el responsable, o para cumplir con medidas precontractuales solicitadas por el interesado.

3.Si la transferencia es necesaria para honrar un contrato a favor del interesado.

4.Si la transparencia es necesaria por razones de interés general.

5.Si la transferencia es necesaria para establecer, ejercitar o defender demandas legales.

6.Si la transferencia es necesaria para proteger los intereses vitales de la persona interesada u otras personas y la persona interesada no puede dar su consentimiento.

7.Si la transferencia procede de un registro cuyo objetivo es proporcionar información al público y que se puede consultar, pero únicamente en la medida en que las leyes relevantes permitan su consulta.

Comisión de Protección de Datos v Facebook Irlanda Ltd y Maximillian Schrems 16 de julio de 2020

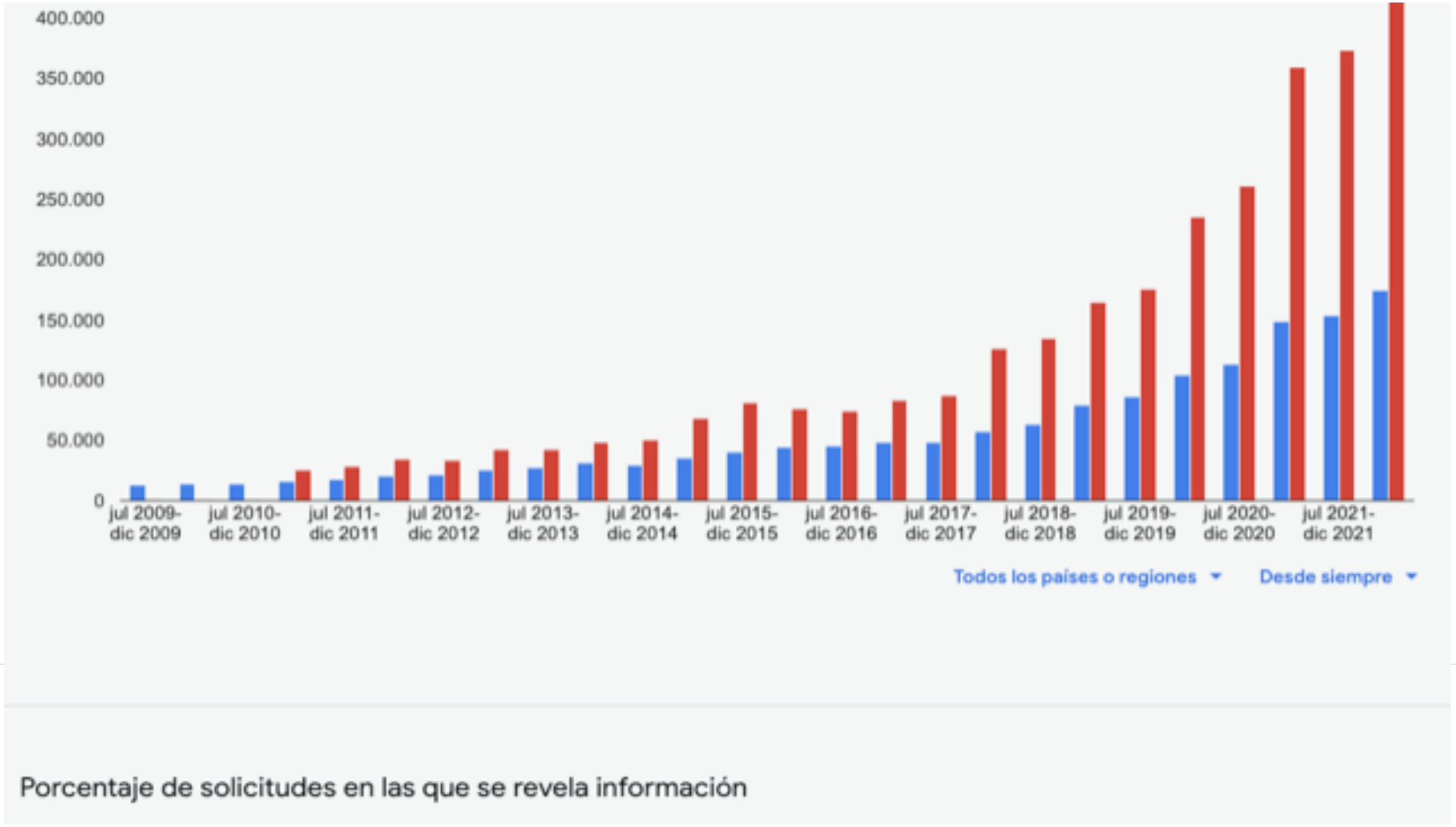
Schrems II, C-311/ 18

- El comisario irlandés de protección de datos solicitó que se invalidaran las cláusulas contractuales tipo para la transferencia de datos personales de Facebook a los Estados Unidos
- El argumento fue que los datos personales se encuentran en tránsito y se almacenan en los Estados Unidos, donde los servicios de inteligencia pueden tener acceso a ellos

Ley de Vigilancia de los EE.UU.

Opinión experta sobre el estado actual de la Ley y las Autoridades de Vigilancia de los EE. UU. del profesor Stephen I. Vladeck, Facultad de Derecho de la Universidad de Texas preparado bajo los auspicios del Comisionado de Berlín para la Protección de Datos y la Libertad de Información en nombre de la Conferencia de Supervisores Independientes de Protección de Datos del Gobierno Federal y los Länder

Informe de transparencia de Google



Informe de transparencia de Google. Metadatos

Solicitudes de información sobre usuarios por motivos de seguridad nacional en Estados Unidos

En este informe de solicitudes de seguridad nacional en Estados Unidos, mostramos por separado las solicitudes procedentes de autoridades estadounidenses que utilizan leyes de seguridad nacional porque estas leyes restringen la cantidad de información que empresas como la nuestra pueden revelar y cuándo pueden revelarla. En casos relacionados con la seguridad nacional, el Gobierno de Estados Unidos puede utilizar la **ley de vigilancia de inteligencia extranjera (FISA)** para solicitar información relacionada o no relacionada con contenido, así como **cartas de seguridad nacional (NSLs)** para solicitar información limitada sobre la identidad de un usuario.

Solicitudes de la FISA no relacionadas con contenido

Las solicitudes de la FISA pueden incluir metadatos no relacionados con contenido como, por ejemplo, los datos de los campos "de" y "para" de una cabecera de correo electrónico o las direcciones IP asociadas a una cuenta determinada.

Periodo de informe	Número de solicitudes	Número de cuentas
ene 2022-jun 2022	Los datos están sujetos a un retraso en el periodo de informe de 6 meses	Los datos están sujetos a un retraso en el periodo de informe de 6 meses
jul 2021-dic 2021	0 – 499	28000 – 28499
ene 2021-jun 2021	0 – 499	27000 – 27499
jul 2020-dic 2020	0 – 499	21500 – 21999

Fuente: Google

Informe de transparencia de Google. Datos de contenido

Solicitudes de la FISA relacionadas con contenido

Las solicitudes de la FISA pueden incluir una petición de contenido sobre usuarios, como mensajes de Gmail, documentos, fotos o vídeos.

Periodo de informe	Número de solicitudes	Número de cuentas
ene 2022-jun 2022	Los datos están sujetos a un retraso en el periodo de informe de 6 meses	Los datos están sujetos a un retraso en el periodo de informe de 6 meses
jul 2021-dic 2021	0 – 499	95500 – 95999
ene 2021-jun 2021	0 – 499	89000 – 89499
jul 2020-dic 2020	0 – 499	80000 – 80499
ene 2020-jun 2020	0 – 499	73500 – 73999
jul 2019-dic 2019	0 – 499	74500 – 74999
ene 2019-jun 2019	0 – 499	69500 – 69999
jul 2018-dic 2018	500 – 999	63000 – 63499
ene 2018-jun 2018	500 – 999	54500 – 54999
jul 2017-dic 2017	500 – 999	44000 – 44499
ene 2017-jun 2017	500 – 999	35000 – 35499
jul 2016-dic 2016	500 – 999	27500 – 27999

Fuente: Google

Conclusión del TJUE

Decisión de adecuación sobre el Escudo de la privacidad

Sobre el poder ilimitado de las agencias de control de los Estados Unidos

- La Decisión 2016/1250 señala la primacía de los requisitos de seguridad nacional de los Estados Unidos, el interés público y la aplicación de la ley y tolera, por tanto, ***la injerencia en los derechos fundamentales de las personas cuyos datos están siendo transferidos a un país tercero***
- Cuando las autoridades públicas utilizan y acceden a datos transferidos desde la UE, la limitación de la protección de datos personales derivada de la legislación de los EE. UU. ***no se circunscribe a satisfacer requisitos equivalentes en esencia a los establecidos por la legislación de la UE*** por el
- ***principio de proporcionalidad***, en tanto en cuanto los programas de control basados en dichas disposiciones ***no se limitan a lo estrictamente necesario***.
- Basándose en las conclusiones de dicha decisión, el TJUE señaló que, en lo que respecta a ***determinados programas de control, dichas disposiciones no indican ninguna limitación a la facultad que confieren para ejecutar dichos programas, ni la existencia de garantías para ciudadanos no estadounidenses a los que potencialmente podrían dirigirse***.

Sobre la falta de derechos aplicables

- A pesar de establecer los requisitos que deben cumplir las autoridades de los Estados Unidos a la hora de realizar programas de seguimiento, ***las disposiciones no otorgan a la persona interesada derechos impugnables ante los tribunales contra las autoridades de los Estados Unidos***.

Sobre la falta de una tutela judicial efectiva

- El mecanismo basado en un Defensor del Pueblo al que se refiere la decisión ***no proporciona a la persona interesada ningún fundamento*** ante ningún órgano que ofrezca garantías sustancialmente equivalentes a las requeridas por el derecho europeo, de forma que se asegure:

a) la independencia del Defensor del Pueblo recogido en el mecanismo y
b) la existencia de normas que capacitan al defensor del Pueblo para adoptar decisiones vinculantes sobre los servicios de inteligencia de los Estados Unidos.

Conclusión del TJUE

Sobre el nivel de protección requerido para una transferencia

Se debe ofrecer al interesado un nivel de protección ***esencialmente equivalente al garantizado dentro de la Unión Europea***, sobre todo en lo que respecta a las salvaguardas adecuadas, los derechos exigibles y la tutela judicial efectiva.

El nivel de protección de terceros países **no es necesario que sea idéntico** al garantizado dentro de la EEE, pero si ser equivalente en esencia.

Comentarios adicionales del Tribunal

•Exportadores de datos: Responsables de **verificar** caso por caso y, cuando sea apropiado, colaborando con el importador del país tercero, **si la ley o la práctica del tercer país repercute sobre la eficacia de las garantías adecuadas incluidas en las herramientas para la transferencia del artículo 46 del RGPD.**

•En estos casos, el Tribunal contempla la posibilidad de que los exportadores **introduzcan medidas adicionales** para colmar estas lagunas de la protección y hacer que alcance el nivel requerido por el derecho de la UE.

•El Tribunal no especifica de qué medidas se trata.

•Esto encaja con el principio de responsabilidad del artículo 5, apartado 2 del RGPD.

Conclusiones del TJUE

Sobre la validez de la decisión 2010/87 (cláusulas contractuales tipo)

Su validez no entra en cuestionamiento por el mero hecho de que las cláusulas contractuales, dada su naturaleza contractual, no son vinculantes para las autoridades del país tercero al que se pueden transferir los datos

La validez depende de:

- Si la decisión incluye un mecanismo efectivo que haga posible, en la práctica, garantizar el cumplimiento con el nivel de protección requerido por el derecho de la UE, y
- Si las transferencias derivadas de dichas cláusulas quedan suspendidas o prohibidas en caso de que se violen las mismas o si es imposible cumplir con ellas.

La decisión 2010/87 establece un mecanismo de este tipo. Obliga a los exportadores de datos y al destinatario de los mismos a verificar, con anterioridad a cualquier transferencia:

- Si el nivel de protección se respeta en el país tercero.
- Si la decisión requiere que el destinatario informe al exportador si por cualquier razón no es capaz de cumplir con las cláusulas contractuales (lo que obligaría al exportador a suspender la transferencia y/o cancelar el contrato con el destinatario).

Medidas suplementarias recomendadas por el CEPD. Junio de 2021. Evaluación completa de la adecuación

*«El alcance de la evaluación se limita a la legislación y las prácticas pertinentes a la protección de los Datos específicos que se transfieren...**a diferencia de lo que sucede con la evaluación completa de adecuación de la Comisión Europea»***

- Fin para el que se transfieren y tratan los datos (RR.HH., mejora de sistemas informáticos (diagnóstico investigación de marketing ensayos clínicos, etc.)
- Tipos de entidades que participan en el tratamiento (públicas/privadas responsable/encargado)
- Sector al que se produce la transferencia (telecomunicaciones, financiero, tecnología publicitaria, etc.)
- Categorías de datos personales transferidos
- Si los datos se almacenan en un país tercero o únicamente se puede acceder remotamente a datos almacenados en la UE/el EEE
- Formato de los datos que se transferirán (texto, encriptados, seudoanonimizados)
- Todos los actores (responsables, encargados, subencargados)
- Posibilidad de que los datos puedan volver a ser transferidos del país tercero a otro país tercero

¿Dónde queda el IMPORTADOR?

Se pasa de una evaluación interna realizada únicamente por el exportador a una enorme participación del importador en la evaluación. Para ello:

- ***Enumerar las leyes y reglamentos del país de destino aplicables al importador o a sus subencargados que permiten el acceso de las autoridades públicas***

- ***A falta de leyes para que las autoridades públicas puedan acceder a los datos, proporcionar información y estadísticas de su experiencia o informes de varias fuentes (socios, código abierto, jurisprudencia nacional, decisión de los órganos de supervisión)***

- ***Indicar qué medidas se han adoptado para prevenir el acceso a los datos transferidos***

  Hace tiempo que Microsoft ha demostrado su compromiso por cumplir y superar los requisitos de las leyes europeas para la protección de datos. Por ejemplo, hemos sido la primera gran empresa tecnológica en comprometernos a cumplir con el RGPD y ampliar los derechos y las protecciones de este reglamento a nuestros clientes en todo el mundo, no solo en la UE. Asimismo, hemos cumplido con las recomendaciones preliminares del Comité Europeo de Protección de Datos (CEDP) relativas a las medidas que deben introducir las empresas como resultado de la sentencia *Schrems II y* hemos hecho pública nuestra iniciativa *Defending Your Data*, que va más allá de las recomendaciones del CEDP. Impugnaremos toda solicitud de cualquier gobierno de que le proporcionemos datos personales de clientes comerciales o del sector público de la UE, siempre y cuando dispongamos de base jurídica para hacerlo. Compensaremos económicamente a los usuarios de nuestros clientes si compartimos datos e infringimos el RGPD causándoles daños.

Fuente: Blog de Microsoft

¿Dónde está el IMPORTADOR?

- ***Proporcionar información detallada de todas las solicitudes de acceso recibidas en un plazo concreto, tipo de datos solicitados, organismo solicitante y en qué medida se compartió la información***

United States national security requests for user information

A variety of laws allow government agencies around the world to request user information for civil, administrative, criminal, and national security purposes. We separately report requests from US authorities using national security laws because these laws restrict how much information companies like us are allowed to share, and when we are allowed to share it. In cases of national security, the US government can use the **Foreign Intelligence Surveillance Act (FISA)** to request non-content and content information, and use **National Security Letters (NSLs)** to request limited information about a user's identity.

Non-content requests under FISA

A FISA request can include non-content metadata—for example, the "from" and "to" fields in an email header and the IP addresses associated with a particular account.

Reporting period	Number of requests	Number of accounts
Jul 2020 – Dec 2020	Data subject to six month reporting delay	Data subject to six month reporting delay
Jan 2020 – Jun 2020	0 – 499	22000 – 22499
Jul 2019 – Dec 2019	0 – 499	30000 – 30499
Jan 2019 – Jun 2019	0 – 499	28500 – 28999

Document was last saved: 19m ago

Content requests under FISA

A FISA request can include a demand for a user's content, such as Gmail messages, documents, photos, and videos.

Reporting period	Number of requests	Number of accounts
Jul 2020 – Dec 2020	Data subject to six month reporting delay	Data subject to six month reporting delay
Jan 2020 – Jun 2020	0 – 499	73500 – 73999
Jul 2019 – Dec 2019	0 – 499	74500 – 74999
Jan 2019 – Jun 2019	0 – 499	69500 – 69999
Jul 2018 – Dec 2018	500 – 999	63000 – 63499
Jan 2018 – Jun 2018	500 – 999	54500 – 54999
Jul 2017 – Dec 2017	500 – 999	44000 – 44499
Jan 2017 – Jun 2017	500 – 999	35000 – 35499
Jul 2016 – Dec 2016	500 – 999	27500 – 27999
Jan 2016 – Jun 2016	500 – 999	22500 – 22999
Jul 2015 – Dec 2015	500 – 999	22500 – 22999

- ***Si el importador no puede compartir dicha información con el exportador (por ejemplo, qué importancia tendría en el caso de una investigación, APD austriaca Google Analytics)***

ANEXO III - POSIBLES FUENTES DE INFORMACION PARA EVALUAR EL PAÍS TERCERO

Concentrarse en la legislación y las prácticas

- ***La legislación del país tercero cumple con la normativa de la UE desde una perspectiva formal, pero en la práctica no se aplica/cumple***

- ***No existe legislación relevante en el país tercero y algunas prácticas son incompatibles con los compromisos de la herramienta para la transferencia***

- ***La legislación del país tercero es problemática (pudiendo tener un impacto sobre la eficacia de la herramienta para la transferencia, los datos transferidos y/o el importador están cubiertos o podrían estar cubiertos por la legislación problemática)***

SUSPENDER LA TRANSFERENCIA o APLICAR MEDIDAS SUPLEMENTARIAS ADECUADAS

RESPONSABLE/ENCARGADO DE DECIDIR SI SUSPENDER, INTRODUCIR MEDIDAS SUPLEMENTARIAS O CONTINUAR CON LA TRANSFERENCIA

EVALUACIÓN VERDADERA
DECISIÓN DOCUMENTADA

NUEVAS cláusulas contractuales tipo

Contexto en que se aplican las cláusulas contractuales tipo y otras herramientas de transferencia mencionadas en el artículo 46 del RGPD.

DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

DECISIÓN DE EJECUCIÓN (UE) 2021/915 DE LA COMISIÓN relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo

Asuntos Google Analytics – ¡No hubo multa!

SEPD - Parlamento Europeo

El SEPD amonestó al Parlamento Europeo por varias violaciones del RPD de la UE, incluyendo aquellos relacionados con transferencias internacionales de datos «dado que se basaba en las cláusulas contractuales tipo cuando no existían pruebas de que los datos personales de las personas interesadas transferidas a los Estados Unidos contaran con un nivel de protección esencial equivalente».

APD de Austria – *Verlangs GmbH* (exportador de datos austríaco)

La APD austriaca concluyó que « la herramienta de *Google Analytics* (al menos la versión del 14 de agosto de 2020) no puede utilizarse en cumplimiento de los requisitos del capítulo V del RGPD». Sin embargo, conforme se ha mencionado anteriormente, la APD concluyó que únicamente el operador de la web (en tanto que exportador de datos) infringió el artículo 44 del RGPD. En este caso, la APD decidió no imponer una multa.

CNIL – Exportador de datos francés

Se requiere al exportador de datos que la actividad de tratamiento de datos con el servicio de *Google Analytics* cumpla con el artículo 4 y los siguientes del RGPD, para lo que debe poner fin a las actividades de tratamiento de datos con la versión actual de la herramienta de *Google Analytics* y proporcionar información al CNIL que demuestre que se ha cumplido con dicha solicitud en el plazo de un mes.

¿Más opciones?

Una APD bávara (BayLDA) solicita a una empresa alemana que deje de utilizar *Mailchimp*

30 de marzo de 2021 Alemania

La sentencia del "Standard" se refiere a un recurso concluido sin medidas formales de supervisión relacionado con la reclamación de un interesado, porque un responsable (una empresa individual) que había utilizado Mailchimp, anunció que actualmente había dejado de usarlo tras nuestra solicitud de información detallada sobre las consecuencias de la decisión *Schrems* II.

Nuestra última notificación al denunciante, en la que aparentemente se basó la publicación, la enviamos a mediados de marzo, e incluía los siguientes fragmentos (de los que proporcionamos una traducción informal):

> «Nos referimos a su reclamación contra... por la violación de la protección de datos al utilizar Mailchimp. Como resultado de nuestra intervención, la empresa nos ha informado de que utilizó Mailchimp en dos ocasiones para enviar boletines informativos. Asimismo, también nos ha informado de que dejará de utilizar Mailchimp de forma inmediata.
>
> La empresa también nos ha hecho saber que únicamente transmitió correos electrónicos a Mailchimp en el contexto anteriormente mencionado. Por otro lado, comenta que la última versión de las recomendaciones del Comité Europeo de Protección de Datos sobre las medidas suplementarias para las transferencias de datos personales a terceros países todavía no está disponible y que todavía se están sometiendo consulta pública. Esto es cierto.
>
> De acuerdo con nuestros análisis, el uso de Mailchimp por parte de ... en los dos casos mencionados (y, con ello, la transferencia de su correo electrónico a Mailchimp, motivo de su reclamación) infringe la ley de protección de datos porque ... no había analizado si además de las cláusulas estándar de protección de datos de la UE (que se utilizaron) era necesario adoptar medidas adicionales en el sentido de la sentencia *Schrems* II del TJE (sentencia C-311/18 de 16/07/2020) para que la transferencia cumpliera con los requisitos de protección de datos. En este asunto había indicios de que, en principio, los servicios de inteligencia estadounidenses podían acceder a los datos a través de Mailchimp basándose en las disposiciones jurídicas de la Ley de Vigilancia de Inteligencia Exterior 702 (50 U.S.C. § 1881) en tanto que proveedor de servicios electrónicos de comunicación y, por tanto, la transferencia sólo sería legítima si se adoptaban dichas medidas adicionales (en caso de que fuera posible y resultaran suficientes para solucionar el problema).»

Marco transatlántico de privacidad de datos

Orden ejecutiva del 7 de octubre de 2022

Dentro del Marco transatlántico de privacidad de datos, los Estados Unidos han asumido unos compromisos sin precedentes.

Por ejemplo, el nuevo marco garantiza que:

- La recopilación de datos de inteligencia **únicamente se puede realizar cuando sea necesario para alcanzar objetivos legítimos para la seguridad nacional y no debe tener un impacto desproporcionado sobre la protección de la privacidad de los individuos y las libertades civiles;**

- Los individuos de la Unión Europea pueden **recurrir a un mecanismo de recurso a varios niveles que incluye un tribunal independiente para el control de la protección de datos** compuesto por individuos que no forman parte del gobierno de los Estados Unidos y que disponen de autoridad plena para pronunciarse sobre las alegaciones y emprender medidas correctivas cuando sea necesario; y

- Las agencias de inteligencia de los Estados Unidos adoptarán **procedimientos para garantizar el control efectivo en las nuevas normas de privacidad y libertades civiles.**

Pasos para adoptar una nueva decisión de adecuación

La Comisión Europea ha elaborado un **Borrador de una nueva decisión de adecuación** – Diciembre de 2022

El CEPD ha elaborado un dictamen sobre el borrador - Febrero de 2023

Parlamento Europeo - Moción para una resolución - Mayo de 2023.

Florina Pop
Profesora Titular
EIPA Maastricht
Correo Electrónico: f.pop@eipa.eu

El contenido de esta publicación representa la opinión del autor y es de su exclusiva responsabilidad. La Comisión Europea no acepta ninguna responsabilidad por el uso que pueda hacerse de la información que contiene

Financiado por
la Unión Europea

EIPA | European Institute of Public Administration