Pridatect

EVALUACIÓN DEL IMPACTO DE LA TRANSFERENCIA

CONTENIDO

1 1

Describa la transferencia1

Identificación del exportador de datos1

por ejemplo, nombre legal y comercial, detalles de registro, país o países exportadores 1

Identificación del importador de datos1

Por ejemplo, nombre legal y comercial, detalles de registro, tipo de receptor (por ejemplo, empresa privada, autoridad pública), país receptor, ¿está sujeto a alguna norma de conducta profesional? 1

Contexto de la transferencia1

Por ejemplo, la naturaleza de la relación entre las partes (por ejemplo, la empresa matriz), la finalidad de la transferencia, los medios de transferencia (por ejemplo, correo electrónico, protocolo de transferencia segura de archivos, acceso remoto), la frecuencia con la que se producirá, qué hará el importador con los datos 1

Categorías, cantidad y formato de los datos personales en cuestión1

por ejemplo, datos de identificación, nacionalidad, currículum de los solicitantes, datos de pago, etc. [Especial relevancia de cualquier dato personal sensible]. 1

Duración de la transferencia1

por ejemplo, indefinido, 1 año, etc. 1

Si hay más de un país de destino o transferencias posteriores relevantes, deberá realizar una Evaluación de Impacto de las Transferencias por separado.1

22

Describa la transferencia2

¿Existen leyes en el país de destino que puedan afectar a la aplicabilidad del instrumento de transferencia del artículo 46 del RGPD seleccionado?2

E.*g. las leyes aplicables en materia de información y acceso por parte de las autoridades públicas competentes, la legislación sectorial aplicable a las particularidades de la transferencia (por ejemplo, sobre datos sanitarios, financieros, de recursos humanos, etc.)* 2

Entra en el ámbito de aplicación de2

1. INTRODUCCIÓN

Tras la decisión del Tribunal de Justicia de la Unión Europea en el caso Schrems II, las organizaciones la Unión Europea que se basan en los mecanismos del artículo 46 del RGPD para transferir datos personales deben evaluar, caso por caso, si las leyes del territorio al
transfieren los datos personales garantizan a los interesados un nivel de
protección de datos esencialmente equivalente al exigido por la legislación de la Unión Europea.

El Consejo Europeo de Protección de Datos (CEPD), en sus "*Recomendaciones 01/2020 sobre las medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE*", propuso las siguientes medidas en relación con la responsabilidad de las transferencias:

1. Conozca sus transferencias ;
2. Identifique los mecanismos de transferencia empleados;
3. **Evalúe si los mecanismos en los que se basa son eficaces para todas las circunstancias de la transferencia;**
4. Adopte medidas complementarias si son necesarias;
5. Implemente medidas complementarias si son necesarias;
6. Reevalúa de forma sistemática los puntos anteriores para comprobar si han cambiado o no.

El objetivo de esta plantilla es proporcionar un marco y un medio para registrar
la evaluación en relación con el paso número 3 de las Recomendaciones 01/2020 del EDPB.

NOTA: Si hay más de un país de destino o una transferencia posterior relevante, deberá realizar una Evaluación del Impacto de la Transferencia por separado para cada paso del ciclo de vida de los datos

1	**Describa la transferencia**
1.1	**Identificación del exportador de datos**
	Por ejemplo, nombre legal y comercial, detalles de registro, país o países exportadores.
1.2	**Identificación del importador de datos**
	Por ejemplo, nombre legal y comercial, detalles de registro, tipo de receptor (por ejemplo, empresa privada, autoridad pública), país receptor, ¿está sujeto a alguna norma de conducta profesional?
1.3	**Contexto de la transferencia**
	Por ejemplo, la naturaleza de la relación entre las partes (por ejemplo, la empresa matriz), la finalidad de la transferencia, los medios de transferencia (por ejemplo, correo electrónico, protocolo de transferencia segura de archivos, acceso remoto), la frecuencia con la que se producirá, qué hará el importador con los datos.
1.4	**Categorías, cantidad y formato de los datos personales objeto de la transferencia**
	Por ejemplo, datos de identificación, nacionalidad, currículum de los solicitantes, datos de pago, etc. [Especial relevancia de cualquier dato personal sensible]. *por ejemplo, número de archivos/registros* *por ejemplo, texto plano, pseudónimo, cifrado, etc.*
1.5	**Nivel de riesgo de perjuicio para los interesados en los casos**

	Por ejemplo, basándose en la información anterior, ¿espera que esta transferencia de datos suponga un nivel de riesgo alto, medio o bajo para los interesados implicados? Esto se reevaluará en la conclusión de esta evaluación de impacto.
1.6	**Duración de la transferencia**
	Por ejemplo, base indefinida, 1 año, etc.

2	**Alternativas**
2.1	**¿Existe alguna alternativa viable de procesador/proveedor que pueda utilizar y que esté ubicada en el EEE/UE o en otro país "adecuado" según el artículo 45 del RGPD?**
	Por ejemplo, puede darse el caso de que pueda encontrar un encargado del tratamiento que cumpla la misma finalidad y que esté situado en Europa y, por tanto, no suponga un riesgo potencial tan grande para los interesados. Si esto no es posible desde el punto de vista financiero, tecnológico u organizativo, explique por qué.
2.2	**¿Puede usted invocar alguna de las excepciones del artículo 49 del RGPD para esta transferencia?**
	Por ejemplo, el interesado ha dado su consentimiento explícito a la transferencia propuesta después de haber sido informado de los posibles riesgos debidos a la ausencia de una decisión de adecuación y de garantías, tal como se indica en el artículo 49 (1) (a). *Por ejemplo, la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la aplicación de medidas precontractuales adoptadas a petición del interesado según el artículo 49 (1) (b).*

	Por ejemplo, la transferencia es necesaria para la celebración o el cumplimiento de un contrato celebrado en interés del interesado entre el responsable del tratamiento y otra persona física o jurídica según el artículo 49 (1) (c). *Por ejemplo, traslado necesario por razones importantes de interés público según el artículo 49 (1) (d).* *Por ejemplo, la transferencia es necesaria para el establecimiento, el ejercicio o la defensa de reclamaciones legales según el artículo 49 (1) (e).* *Por ejemplo, la transferencia es necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado está física o legalmente incapacitado para dar su consentimiento según el artículo 49 (1) (f).* *Por ejemplo, la transferencia realizada desde un registro público según el artículo 49 (1) (g) y 49 (2).*

3	**Describa el régimen jurídico del país del importador**
3.1	**¿Ofrece la legislación del país del importador un nivel de protección de datos esencialmente equivalente al garantizado en la UE/EEE por el RGPD?**
	Por ejemplo, entre los factores relevantes a la hora de realizar esta evaluación se encuentran el Estado de Derecho; el respeto de los derechos humanos y las libertades fundamentales; la legislación pertinente; el acceso de las autoridades públicas a los datos personales; la existencia de autoridades de control independientes; los derechos efectivos de los interesados y la reparación efectiva de los interesados cuyos datos personales se transfieren. *Otros factores que indican preocupación podrían ser: el no reconocimiento o ejecución de sentencias o laudos arbitrales extranjeros, que el país no sea parte de convenios internacionales (por ejemplo, de derechos humanos), el acceso limitado a la justicia para los litigantes extranjeros, autoridades no independientes o no imparciales, niveles generalizados de corrupción, etc.*
3.2	**¿Existen leyes específicas en el país de destino que puedan afectar a la aplicabilidad del instrumento de transferencia del artículo 46 del RGPD seleccionado?**
	Por ejemplo, la legislación aplicable en materia de información y acceso por parte de las autoridades públicas competentes, la legislación sectorial

	aplicable a las particularidades de la transferencia (por ejemplo, sobre datos sanitarios, financieros, de recursos humanos, etc.) *Por ejemplo, la legislación estadounidense Sección 702 FISA y la Orden Ejecutiva 12 333.* *por ejemplo, el sistema SORM de Rusia (Система оперативно-разыскных мероприятий, lit. '*Sistema *de Actividades Operativas de Investigación, tal y como se recoge en el TEDH en el caso Zakharov v. Russian Federation, no. 47143/06, TEDH 2009-X, apartado 302)*
3.3	**En caso afirmativo, ¿entra el importador de datos en el ámbito de aplicación de dichas leyes?**
	Por ejemplo, usted utiliza una herramienta de gestión de recursos humanos que está domiciliada en Estados Unidos, por lo que está llevando a cabo esta evaluación, pero la FISA + EO 12.333 no tiene como objetivo -por ejemplo- los datos de recursos humanos. Así lo confirma un informe del Privacy and Civil Liberty Oversight Board (PCLOB) (aquí), así como las decisiones del Foreign Intelligence Surveillance Court (FISC) al conceder el acceso en casos FISA (aquí). *Estas fuentes no contienen ninguna indicación de que dichos datos hayan sido alguna vez objeto de búsquedas en virtud del artículo 702 de la FISA o de la OE 12.333. Además, el artículo 702 de la FISA sólo se refiere a los servicios de comunicaciones prestados a los objetivos de las búsquedas, y no a otros o a solicitudes como la presente. Por lo tanto, aquí se declararía que se cree que la probabilidad de que la empresa matriz tenga o reciba una orden de vigilancia con respecto a sus datos durante el período considerado es muy baja.* *Esto sólo puede justificarse en la medida en que haya información pública disponible.*
3.4	**¿Se puede hacer la solicitud con la falta de revisión judicial?**

	Por ejemplo, no hay ningún requisito obligatorio de supervisión judicial a través de un juez. Por ejemplo, en EE.UU. las Cartas de Seguridad Nacional (NSL) no requieren la firma de un juez antes de que se ejecute la orden de mordaza/solicitud de acceso. Aunque las propias solicitudes pueden estar ocultas para todos, excepto para el destinatario, los datos sobre el número de solicitudes realizadas por la autoridad pública en un periodo de tiempo probablemente estarán disponibles públicamente.
3.5	**¿Proporciona la ley al importador de datos algún mecanismo para impugnar la aplicación de dichas leyes a los datos personales?**
	Por ejemplo, con los mecanismos no judiciales esto es poco probable. Un ejemplo de impugnación podría ser una acción judicial ante el tribunal competente con el objetivo de detener o controlar el acceso de las autoridades a los datos personales.
3.6	**¿Prevé la ley medidas técnicas obligatorias que hagan posible el acceso de las Autoridades Públicas a los datos personales?**
	Por ejemplo, puertas traseras obligatorias en los programas informáticos que se utilizarán en el tratamiento de datos.
3.7	**¿Prevé la ley el acceso a los datos en transferencia?**
	Por ejemplo, ¿hay un registro de acceso a los proveedores de telecomunicaciones en el país importador que pueda afectar a sus datos antes de que el importador los reciba?

4	**Describa la probabilidad de que la legislación se aplique a su transferencia de datos personales**

4.1	**¿Han solicitado previamente las Autoridades Públicas el acceso a los datos personales que posee el importador de datos?**
	Por ejemplo, colaborar con el importador para saber si ha recibido alguna solicitud de acceso.
4.2	**¿Han conseguido las Autoridades Públicas acceder a los datos personales que posee el importador de datos en el pasado?**
	Por ejemplo, ¿ha tenido éxito alguna solicitud?
4.3	**¿Ha conseguido el importador de datos que la Autoridad Pública renuncie a su solicitud de datos en el pasado?**
	Por ejemplo, algunos países en los que se fomenta la impugnación de las solicitudes pueden dar lugar a una denegación. Esto es una consideración: si el importador recibe una solicitud, ¿hay alguna posibilidad de que pueda obligar a la autoridad a renunciar a la solicitud de acceso?
4.4	**¿Han solicitado las Autoridades Públicas anteriormente el acceso a los datos de la misma categoría de empresa que usted conoce?**
	Por ejemplo, aunque el importador no haya recibido ninguna solicitud, o esté bajo una orden que prohíba su divulgación, puede ser útil buscar en otras empresas del sector. Los datos suelen estar disponibles públicamente en los proveedores más importantes.
4.5	**¿Tiene el país del importador de datos algún sistema para prohibir la divulgación de las solicitudes de acceso?**
	Por ejemplo, algunas autoridades públicas incluirán órdenes de mordaza o acuerdos de confidencialidad con sus solicitudes de acceso, lo que significa que

	el importador de datos puede haber recibido solicitudes, pero no puede compartir esta información con usted.
4.6	**¿Sabe si sus datos contienen potencialmente algún "selector" específico, o atributo de identificación, que pueda ser de interés para las Autoridades Públicas del país importador?**
	Por ejemplo, ¿es probable que sus datos contengan algo relacionado con un nombre, un correo electrónico, etc. que pueda ser marcado para una vigilancia o un acceso adicional? Podría ser un selector duro (correo electrónico de una persona de interés) o un selector blando (ubicación geográfica o nodo específico conocido por su actividad delictiva). Se pueden encontrar más ejemplos y detalles en la infografía del Director de Inteligencia Nacional aquí.

5	**Salvaguardas**
5.1	**¿Es necesaria la transmisión de texto plano en la transmisión de esta transferencia?**
	Por ejemplo, algunas actividades de tratamiento requieren que los datos se transmitan en formato de texto plano (no cifrado).
5.2	**¿Es necesario el tratamiento de texto plano tras la recepción de los datos personales?**
	Por ejemplo, algunas actividades de tratamiento requieren que los datos se reciban en formato de texto plano (no cifrado). Por ejemplo, los datos de recursos humanos que se introducen en un sistema de gestión de recursos humanos si están codificados son esencialmente inútiles, ya que no se ajustan a los campos de entrada.
5.3	**¿Está el receptor contractualmente obligado a defender los datos personales en cuestión contra las solicitudes de acceso?**

	Por ejemplo, en la UE, los importadores tienen un deber general de diligencia que les obliga a defender los datos personales de los ciudadanos. Esto no siempre aplica a otros países.
5.4	**¿Ha implementado algún control adicional de acceso al cifrado con el fin de minimizar la probabilidad de que se produzca una infracción o de reducir el riesgo de daño al sujeto de los datos si se produce una infracción?**
	Por ejemplo, en la encriptación en reposo se encriptan los datos antes de la transferencia utilizando una solución de encriptación adecuada (es decir, encriptación de almacenamiento) y se aplican procedimientos adecuados de gestión de claves. Una solución superior sería cifrar los datos antes de la transferencia utilizando soluciones de cifrado apropiadas y luego dividir los conjuntos de datos cifrados entre varias partes.
5.5	**¿Ha aplicado el principio de minimización de datos?**
	Por ejemplo, usted minimiza los datos transferidos al mínimo necesario para llevar a cabo la actividad de tratamiento. Esto también podría incluir técnicas de seudonimización antes de la transferencia, sin que el importador tenga acceso a la información adicional. Una solución superior sería dividir los conjuntos de datos seudonimizados entre múltiples entidades, de modo que haya un riesgo mínimo de que cualquiera de las partes pueda identificar a un sujeto de datos.
5.6	**¿Ha establecido el importador de datos alguna medida de control de acceso de la organización?**
	Por ejemplo, podría incluir perfiles de acceso basados en funciones, protocolos de acceso de terceros o una política para gestionar las órdenes legales de acceso a datos de terceros.

5.7	**¿Ha establecido el importador/exportador de datos un proceso para gestionar las reclamaciones de los interesados que incluya un sistema de compensación?**
	Por ejemplo, no es estrictamente necesario y sólo está al alcance de las organizaciones más grandes con importantes recursos financieros,
5.8	**¿Ha establecido algún derecho contractual para que los interesados puedan presentar una reclamación contra el exportador si éste no cumple con sus obligaciones?**
	Por ejemplo, podría establecerse una política para garantizar que estos casos se traten de forma eficaz. Los derechos contractuales podrían incluirse en los principales acuerdos de servicio.
5.9	**¿Existe alguna autoridad de protección de datos con poderes activos de supervisión sobre el importador y/o exportador de datos?**
	Por ejemplo, algunos países pueden tener una autoridad de protección de datos más activa que puede proporcionar protecciones en las que se puede confiar. Esto puede salvaguardar los derechos de los interesados y es positivo para el éxito de la transferencia.
5.10	**¿Dispone de algún procedimiento de revisión para garantizar que las descripciones contenidas en este documento siguen siendo exactas?**
	Por ejemplo, es importante asegurarse de que se dispone de un procedimiento de revisión. Los datos recogidos de fuentes públicas en el marco de esta evaluación de impacto pueden quedar obsoletos en cuestión de meses o años. La revisión periódica garantiza que los interesados no corran peligro.

Conclusión:

Permitido	*No se permite*

(Elimine el color de la casilla que no corresponda)

Su traslado debería ser permitido una vez que haya completado la evaluación anterior y crea que las respuestas indican que lo es:

- *Cumplir con los requisitos más amplios del RGPD de la UE*
- *Confirmar que la transferencia no es de alto riesgo o compleja*
- *Evaluar y registrar los detalles de la transferencia restringida (Secciones 1-2)*
- *Confirmar que es probable que los derechos contractuales establecidos en su herramienta de transferencia sean ejecutables en el país de destino (secciones 3 y 4), y que, cuando haya dudas, el riesgo de daño a los interesados sea bajo o pueda reducirse a bajo mediante pasos y medidas adicionales, como el cifrado, la seudonimización, etc. (sección 5).*
- *Confirme que una de las siguientes opciones es aplicable en el contexto de su transferencia restringida:*
    1. *el régimen de destino proporciona protecciones adecuadas para el acceso de terceros a los datos (incluida la vigilancia).*
    2. *la probabilidad de que se produzca el acceso de terceros (incluida la vigilancia) es mínima o se convierte en mínima una vez que se aplican medidas o protecciones adicionales.*
    3. *si se produce un acceso a los datos por parte de terceros, el riesgo de perjuicio para los interesados es bajo o se convierte en bajo una vez que se aplican medidas o protecciones adicionales.*

Al justificar la conclusión en esta sección, remítase a sus respuestas en las secciones 1-5.