

Speaking points

Evento: Jornada sobre incidencia de la legislación sobre protección de datos en el intercambio de información empleo/servicios sociales

Fecha: 6 de julio 2021

Hora: 10.45 a 11.10

Formato: 10 minutos ponencia + 10 minutos preguntas

Introducción

- Agradecer la invitación a esta charla
- Poner en valor que el área de empleo y servicios sociales es un ámbito en el que se gestiona una gran cantidad de datos personales sensibles y, por tanto, es fundamental que los instrumentos de intercambio de información cuenten con **todas las garantías necesarias.**
- A su vez, **es importante facilitar el intercambio** de datos entre administraciones y entre éstas con las ONG., ya que de ello depende en gran medida que el interesado pueda encontrar un empleo que se ajuste a su perfil y que resulte en última instancia en una más fácil y **mejor inclusión social de la persona.**

Marco regulatorio europeo para flujos de datos personales dentro de la Unión Europea

- El marco europeo de protección de datos viene establecido por el Reglamento general de protección de datos¹. Al tratarse de un reglamento, sus normas son directamente aplicables en todos los Estados Miembros, con lo que nos aseguramos que **dentro de la Unión Europea, el standard de garantías en materia de protección de datos y de transferencias es el mismo.**
- Esta normativa parte de una serie de principios relativos al tratamiento, establecidos en su Artículo 5, a saber (1) licitud, lealtad y transparencia, (2) limitación de la finalidad; (3) minimización de datos; (4) exactitud; (5) limitación del plazo de conservación;

¹) REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- Todo tratamiento de los datos, incluyendo el intercambio, será lícito únicamente si se justifica en una de las bases legales que establece el Artículo 6 del RGPD, es decir,

- si el interesado dio su consentimiento;

- el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte, el cumplimiento de una obligación legal o para proteger intereses vitales del interesado o de otra persona física;

- el tratamiento es necesario por interés público o en el ejercicio de poderes públicos o para la satisfacción de intereses legítimos;

- La falta de una base legal en el intercambio de datos supone el incumplimiento del RGPD. Por eso, **el aviso de privacidad** es clave en el procesamiento de datos, ya que este indicará a los sujetos del procesamiento las características principales del tratamiento al que serán sometidos los datos personales, así como la posibilidad de ejercer los derechos ARCO (acceso, rectificación, cancelación y oposición).

- En el aviso de privacidad deberá indicarse asimismo **quienes serán los receptores** de los datos, incluyendo posibles transferencias a otras administraciones de Estados Miembros o terceros países, y sobre qué base legal.

- Otro de los elementos clave para asegurar el cumplimiento del RGPD en el intercambio de información con otras administraciones públicas europeas es el **principio de la protección de datos desde el diseño y por defecto**. De acuerdo con este principio, teniendo en cuenta el estado de la técnica y los riesgos del tratamiento, los responsables del tratamiento deberán **adoptar medidas técnicas y organizativas apropiadas**, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento.

- Una vez que sabemos que conocemos que, dentro de la Unión Europea, las transferencias de datos están sujetas a las mismas garantías que una transferencia nacional debido al instrumento normativo del Reglamento, veremos a continuación los instrumentos del RGPD para transferencias de datos a terceros países o a organizaciones internacionales.

Marco regulatorio europeo para los flujos de datos personales a terceros países u organizaciones internacionales

- El marco normativo europeo para las transferencias de datos personales a terceros países u organizaciones internacionales viene regulado en el **Capítulo V del RGPD** en sus **artículos 44 a 50**, completado con la **interpretación que realiza el Tribunal de Justicia de la Unión Europea (TJUE)** de sus preceptos y las directrices sobre su aplicación emitidas por el Consejo Europeo de Protección de Datos.
- Como punto de partida para las transferencias internacionales, cabe señalar que la Comisión Europea tiene competencias para determinar, de conformidad con el artículo 45 del RGPD, **si un país fuera de la Unión Europea** ofrece un nivel adecuado de protección de datos, a través de la llamada “**Decisión de Adecuación**”. En particular, la adopción de una decisión de adecuación implica una propuesta de la Comisión, un dictamen del CEPD, una aprobación de los representantes de los países de la UE y, por último, la adopción de la decisión por parte de la Comisión Europea. El efecto de esta decisión es que los datos personales pueden transmitirse de la UE (y Noruega, Liechtenstein e Islandia) a ese tercer país sin necesidad de ninguna otra salvaguardia. En otras palabras, las transferencias al país en cuestión se asimilarán a las transmisiones de datos dentro de la UE².
- Podríamos decir que tras la reciente sentencia por la que se invalidó el Escudo de la Privacidad o sentencia Schrems II³, son tiempos complejos para las transferencias internacionales. No obstante, aunque es cierto que **el margen de maniobra para garantizar la fluidez de los flujos de datos entre Estados Unidos y la UE se ha reducido sustancialmente**, todavía no es el final de los flujos internacionales de datos. Las transferencias a los Estados Unidos siguen siendo posibles en determinadas condiciones.
- Con la sentencia Schrems II, el TJUE invalidó el Escudo de la privacidad, sobre la base de (i) la falta de proporcionalidad causada por los programas de vigilancia masiva y (ii) la falta de vías de recurso efectivas (de una manera no específica) en los Estados Unidos.

² Hasta la fecha, la Comisión ha reconocido que Andorra, Argentina, Canadá (organizaciones comerciales), las Islas Feroe, Guernesey, Israel, la Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay ofrecen una protección adecuada.

³ (Sentencia en el asunto C-311/18, Data Protection Commissioner/Maximillian Schrems y Facebook Ireland)

- Esta sentencia tiene enormes **implicaciones para todas las transferencias a todos los países**, no solo a los Estados Unidos, ya que el TJUE también exigió en la misma un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en el seno de la Unión Europea, con independencia de la base utilizada para transferir los datos.

- A resultas de la sentencia Schrems II, se plantean actualmente **dos retos principales**:

(1) **por parte de la Comisión Europea**, asegurar que todas las decisiones de adecuación del marco de protección de datos de terceros países tienen en cuenta la nueva jurisprudencia y son conformes a sus directrices interpretativas.

(2) **por parte de los operadores económicos** que realizan actividades con tratamiento de datos en la Unión Europea, cumplir con los requisitos legales cuando no exista decisión de adecuación para las transferencias a un tercer país. Esto implica una evaluación caso por caso de los riesgos de dicha transferencia y la adopción de salvaguardas, bien sea a través de la adopción de las Cláusulas Contractuales Estándar publicadas por la Comisión Europea, o bien a través de la adopción de medidas contractuales a estos efectos.

[El marco actual de los flujos internacionales de datos en el marco de la Unión Europea](#)

- Al eliminarse el Escudo de la privacidad, **las cláusulas contractuales tipo (CCT)** son, en la práctica, la principal herramienta restante para continuar, en cierta medida, la transferencia de datos a los Estados Unidos. La buena noticia es que **las nuevas CCT propuestas por la Comisión el 4 de junio de 2021** presentan globalmente un nivel de protección más elevado para los interesados. Esto debería facilitar la compleja evaluación del cumplimiento que los responsables del tratamiento deben llevar a cabo para seguir transfiriendo datos a los EE. UU.

- Como hemos comentado antes, en la sentencia Schrems II, el TJUE dictaminó que las transferencias basadas en garantías adecuadas deben garantizar un nivel de protección esencialmente equivalente al garantizado en la UE, añadiendo, en su caso, **medidas complementarias a dichas garantías adecuadas**.

- El Consejo Europeo de Protección de Datos (CEPD) formuló en noviembre de 2020 **recomendaciones sobre estas medidas complementarias⁴, en las que enumeraba seis etapas⁵** diferentes en cualquier transferencia internacional:

- **La evaluación de estas medidas requiere un análisis caso por caso**, y no existe por tanto, una “bala de plata” para las empresas que tienen que realizar la evaluación y aplicar las salvaguardias, cuando, en última instancia, la transferencia propiamente dicha no está prohibida. Tampoco existe una solución fácil para los terceros países que desean facilitar los flujos transfronterizos de datos y que tienen una legislación inadecuada.

⁴ Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020

⁵ Las seis etapas son:

1. conocer sus transferencias;
2. identificar las herramientas de transferencia en las que se basa;
3. evaluar si la herramienta de transferencia es eficaz

Este es el paso clave: La evaluación debe tener en cuenta la legislación del tercer país de destino y si la transferencia en cuestión entra en su ámbito de aplicación, así como cualquier posible práctica ilegal. A continuación, si la herramienta de transferencia no puede aplicarse eficazmente, se necesitan medidas complementarias, de lo contrario, no podrá realizarse ninguna transferencia.

4. adoptar medidas complementarias adecuadas (de carácter técnico, contractual u organizativo);
5. fases del procedimiento una vez identificadas las medidas complementarias;
6. reevaluar periódicamente.