GUÍA BÁSICA PARA LA ADPTACIÓN AL REGLAMENTO DE LA LOPD

WWW.MITTUM.COM

MITTUM

MITTUM

1. ¿Cuándo empezar la adaptación?

El nuevo **Reglamento General de Protección de Datos** (RGPD) entró en vigor en mayo de 2016 y será **aplicable a partir de mayo de 2018**.

No obstante, en el periodo de transición es imprescindible preparar y adoptar las medidas necesarias asegurar el cumplimiento de las previsiones del RGPD en el momento en que sea de aplicación.

Conforme se adelanta en la **Guía del Reglamento General de Protección de Datos para responsables de tratamiento** publicada por la AEPD, muchas de las recomendaciones o interpretaciones que ofrece pueden ponerse en práctica de inmediato porque tienen que ver con **actuaciones que debieran iniciarse ya durante el periodo de transición** entre la entrada en vigor y el inicio de la aplicación del RGPD.

MITTUM

Siguiendo las recomendaciones de la Guía, destacamos las cuestiones más relevantes para las empresas:

LETSLAW

MITTUM

Principio de responsabilidad proactiva

Se exige una **actitud consciente, diligente y proactiva** por parte de las empresas, que deberán analizar todos los tratamientos de datos personales que llevan a cabo para determinar la forma en que aplicarán las medidas que el RGPD prevé. Será importante asegurarse de que son las medidas adecuadas y que así puede demostrarse ante los interesados y autoridades de supervisión.

LETSLAW

El enfoque de riesgo

Será imprescindible realizar un **análisis de los riesgos particulares de cada empresa**. La aplicación del RGPD dependerá de las características de cada empresa, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

MITTUM

2. BASE DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS:

LETSLAW

MITTUM

2.1 Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos:

• Incluir la **base legal sobre la que se desarrolla el tratamiento** en el momento de recoger los datos de los interesados.

• Especificar y documentar los **intereses legítimos en que se fundamentan las operaciones de tratamiento** en casos como las Evaluaciones de Impacto sobre la Protección de Datos o en determinadas transferencias internacionales.

LETSLAW

MITTUM

2.2 El consentimiento debe ser “inequívoco”

El **consentimiento, además de inequívoco**, ha de ser **explícito** en el caso de:

- Tratamiento de datos sensibles
- Adopción de decisiones automatizadas
- Transferencias internacionales

En estos casos no cabrá deducir el consentimiento de una acción del interesado, sino que deberá ser explícito.

Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que se hayan prestado mediante una manifestación o acción afirmativa (no serán válidos los consentimientos obtenidos de forma tácita).

IMPORTANTE: No seguir obteniendo consentimientos por omisión y revisar esos tratamientos para que se adecuen a las previsiones del RGPD.

La **adaptación** puede llevarse a cabo:

- Obteniendo un consentimiento de los interesados acorde con el RGPD.
- Valorando si los tratamientos afectados pueden apoyarse en otra base legal.

LETSLAW

MITTUM

3. TRANSPARENCIA E INFORMACIÓN A LOS INTERESADOS:

LETSLAW

MITTUM

3. Transparencia e información a los interesados:

Toda la información que se facilite a los interesados deberá ser **concisa, transparente, inteligible** y de **fácil acceso**, con un **lenguaje claro y sencillo**. Además de proporcionarse en modo expreso, preciso e inequívoco como indica ya la LOPD.

La información deberá facilitarse **por escrito, incluidos los medios electrónicos** cuando sea apropiado.

Se **amplía el contenido de la información** que debe proporcionarse, incluyendo:

- Base jurídica del tratamiento
- Intención de realizar transferencias internacionales
- Datos del Delegado de Protección de Datos (Data Protection Officer, “DPO”).
- Elaboración de perfiles

LETSLAW

MITTUM

4. NUEVOS DERECHOS:

LETSLAW

MITTUM

4. Nuevos derechos:

Procedimiento para el ejercicio y obligaciones:

- Facilitar a los interesados el ejercicio de sus derechos, y los **procedimientos** y las formas para ello deben ser **visibles, accesibles y sencillos** (posibilitar solicitud por medios telemáticos)

- El ejercicio será **gratuito para el interesado** (excepto solicitudes repetitivas, excesivas, o infundadas cuando así lo demuestre el responsable.)

- Articular **procedimientos que permitan fácilmente acreditar a los interesados que han ejercido sus derechos por medios electrónicos**.

- Informar al interesado en el **plazo de 1 mes** (aunque sea para informar de la negativa de atender la solicitud).

MITTUM

4. Nuevos derechos:

Derecho al acceso:

- El interesado tiene derecho a obtener **una copia de los datos personales** objeto del tratamiento.

Se cumplirá con este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

LETSLAW

MITTUM

4. Nuevos derechos:

Derecho al olvido:

- No es un derecho separado de los derechos ARCO, **sino la consecuencia del ejercicio de los derechos de cancelación u oposición en el entorno online**, que dará lugar al **borrado** de los datos personales.

Los responsables que hayan hecho públicos los datos personales deberán adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar sus datos.

LETSLAW

MITTUM

4. Nuevos derechos:

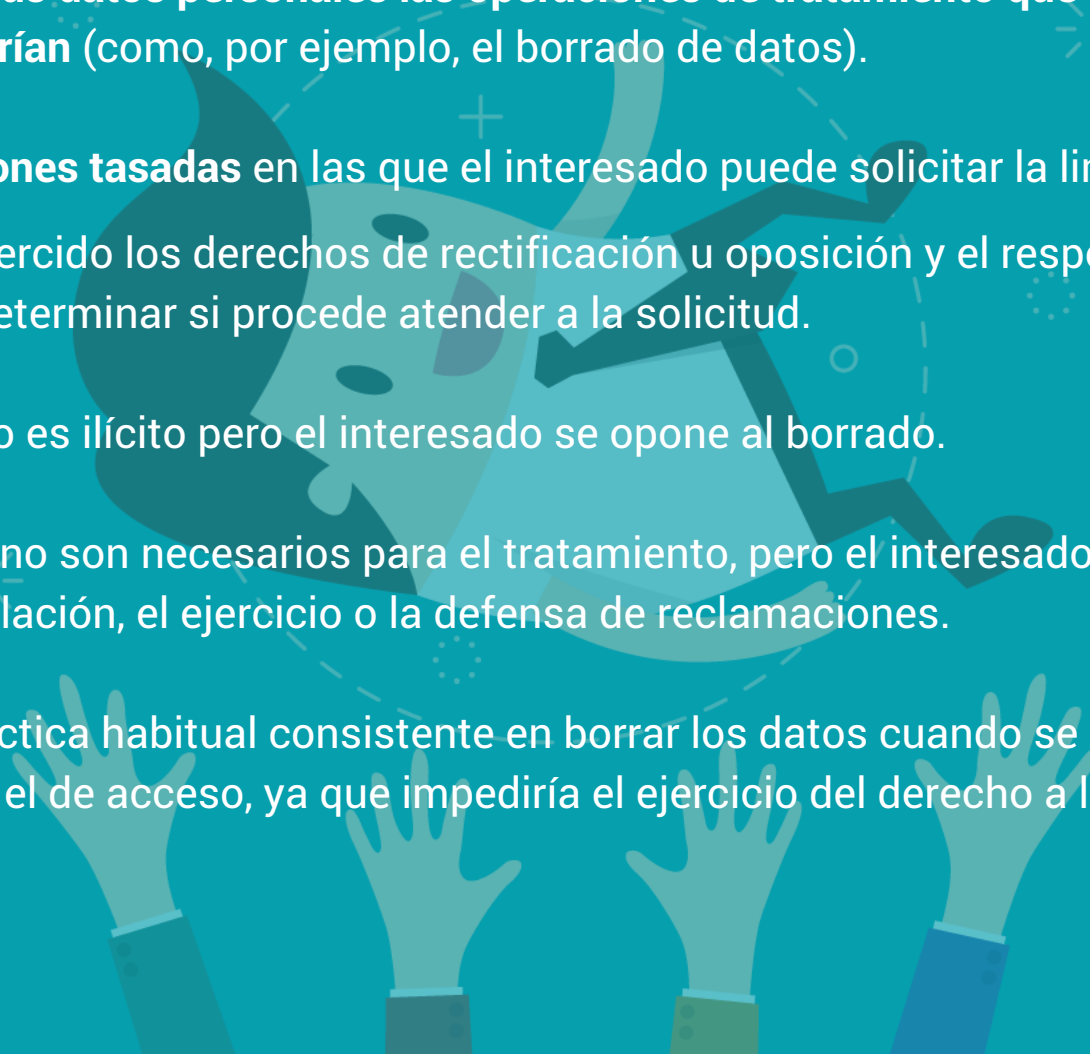
Limitación del tratamiento:

- Es un derecho de los interesados a través del cual pueden **solicitar que no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían** (como, por ejemplo, el borrado de datos).

Se fijan **situaciones tasadas** en las que el interesado puede solicitar la limitación:

- Cuando ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito pero el interesado se opone al borrado.
- Los datos ya no son necesarios para el tratamiento, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

Se impide la práctica habitual consistente en borrar los datos cuando se ejercitan otros derechos, como el de acceso, ya que impediría el ejercicio del derecho a la limitación del tratamiento.



LETSLAW

MITTUM

4. Nuevos derechos:

Derecho a la portabilidad

Cuando el interesado ejercite el derecho de acceso deberá proporcionarle **copia en un formato estructurado, de uso común y lectura mecánica**. Los datos se transmitirán **directamente de un responsable a otro**, sin necesidad de que sean transmitidos previamente al propio interesado, si es técnicamente posible.

Este derecho sólo puede ejercerse cuando el tratamiento:

- Sea automatizado.
- Se base en el consentimiento o en un contrato.
- Respecto de los datos proporcionados al responsable y que conciernan al interesado, incluidos los datos derivados de la propia actividad del interesado.

MITTUM

5. RELACIONES RESPONSABLE-ENCARGADO:

LETSLAW

Aunque la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, el RGPD contiene **obligaciones expresamente dirigidas a los encargados**.

5.1 Nuevas obligaciones específicas para los encargados:

- Mantener un **registro de actividades de tratamiento**.
- **Determinar las medidas de seguridad aplicables** a los tratamientos que realizan.
- Designar a un **DPO** en los casos previstos por el RGPD.

5.2 Elección del encargado del tratamiento:

- IMPORTANTE: Los **responsables habrán adoptar medidas apropiadas y elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas**, de manera que el tratamiento sea conforme con los requisitos del RGPD. Lo mismo se exigirá a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

- Los encargados podrán adherirse a có**digos de conducta o certificarse** para demostrar que ofrecen las garantías necesarias.

MITTUM

5.3 Contenido del contrato de encargado de tratamiento:

- Las relaciones entre el responsable y el encargado deben **formalizarse en un contrato o en un acto jurídico**.

- Se fija un **contenido mínimo de los contratos de encargo**, entre otros se exige:
    - Objeto, duración, naturaleza y la finalidad del tratamiento.
    - Tipo de datos personales y categorías de interesados.
    - Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
    - Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones.
    - Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados...

MITTUM

IMPORTANTE: **Los contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse** incluyendo el contenido mínimo. No serán sean válidas las remisiones genéricas al artículo del RGPD que los regula.

LETSLAW

MITTUM

6. MEDIDAS DE RESPONSABILIDAD ACTIVA:

LETSLAW

MITTUM

6.1 Análisis de riesgo:

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos)

- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

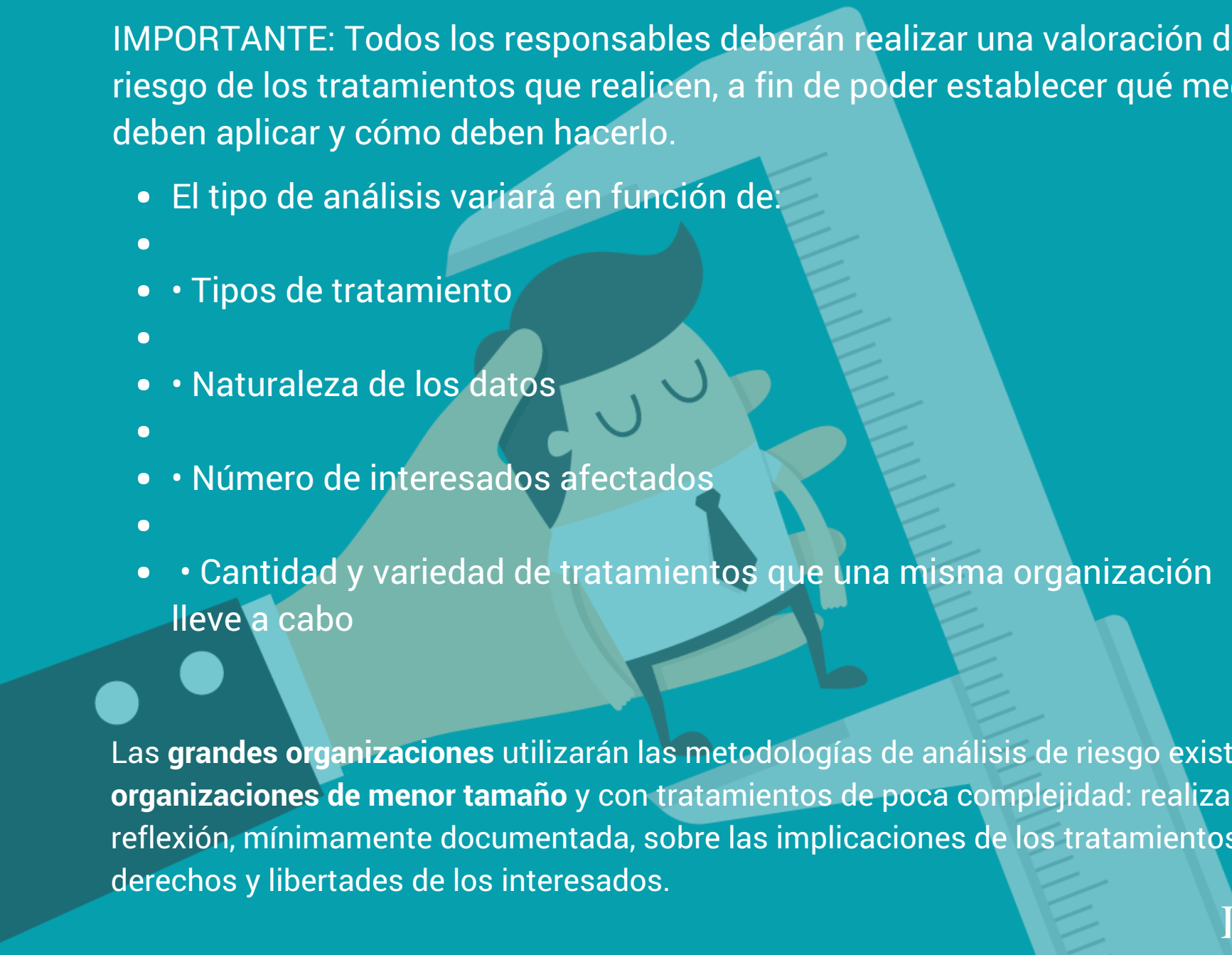
LETSLAW

MITTUM

6.1 Análisis de riesgo:

IMPORTANTE: Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

- El tipo de análisis variará en función de:
-
- • Tipos de tratamiento
-
- • Naturaleza de los datos
-
- • Número de interesados afectados
-
- • Cantidad y variedad de tratamientos que una misma organización lleve a cabo



Las **grandes organizaciones** utilizarán las metodologías de análisis de riesgo existentes. Las **organizaciones de menor tamaño** y con tratamientos de poca complejidad: realizarán una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

LETSLAW

MITTUM

6.2 Registro de actividades de tratamiento

IMPORTANTE: **Responsables y encargados deberán mantener un registro de operaciones de tratamiento** en el que se contenga la información que establece el RGPD, indicando cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del DPO
- Finalidades del tratamiento
- Descripción de categorías de interesados y categorías de datos personales tratados
- Transferencias internacionales de datos...

LETSLAW

6.2 Registro de actividades de tratamiento

Están exentas las empresas con menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

6.3 Protección de datos desde el diseño y por defecto

Con **anterioridad al inicio del tratamiento y cuando se esté desarrollando**, los responsables deberán adoptar medidas técnicas y organizativas que:

- Permitan aplicar de forma efectiva los principios del RGPD
- Garanticen que solo se tratan los datos necesarios

6.4 Medidas de seguridad

En el RGPD, los responsables y encargados establecerán las **medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado** en función de los riesgos detectados en el análisis previo. El RGPD pide que se tomen en consideración más variables:

- El coste de la técnica
- Los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento
- Los riesgos para los derechos y libertades

IMPORTANTE: **Las medidas de seguridad previstas en el Reglamento de la LOPD no serán válidas de forma automática**. Según los resultados del análisis de riesgos previo, se conocerá si las medidas actuales son las adecuadas o si deben tomarse medidas adicionales o prescindir de alguna.

6.5 Notificación de violaciones de seguridad de los datos

El **RGPD define las quiebras de seguridad de una forma muy amplia** (por ejemplo, el acceso no autorizado a una base de datos por el personal de una empresa o el borrado accidental son considerados violaciones de seguridad).

La **valoración del riesgo de la quiebra es distinta del análisis de riesgos previo a todo tratamiento**. Debe establecerse las consecuencias que la violación de seguridad puede tener, por sus características y el tipo de datos a que se refiere, para los interesados, determinando si supone un daño en sus derechos o libertades

- **Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad competente**, a menos que sea improbable poner en riesgo los derechos y libertades de los afectados, sin dilación indebida y, a ser posible, en un plazo de **72 horas** desde que se conoce.

6.6 Notificación de violaciones de seguridad de los datos

- Cuando además suponga un **alto riesgo para los interesados** y pueda ocasionar daños de entidad habrá que **notificárselo también a éstos** para que puedan reaccionar y protegerse de sus consecuencias.

La **AEPD** adaptará el **canal** específico para la notificación de las quiebras de seguridad en el ámbito de las comunicaciones electrónicas **para que pueda ser utilizado para la comunicación de todas las violaciones de seguridad**.

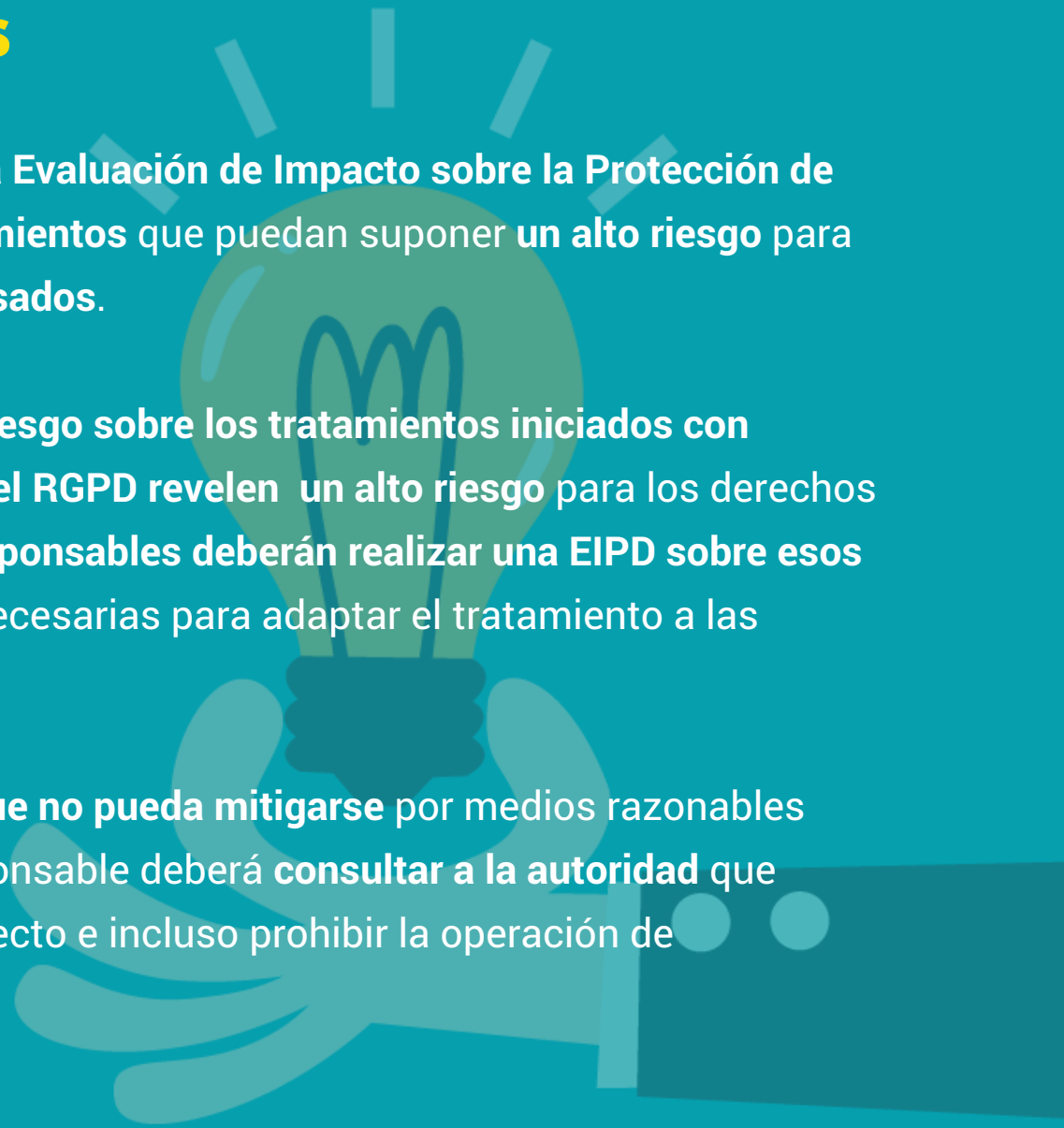
El Grupo del **Artículo 29** preparará un **formulario estandarizado** a nivel europeo tanto para ayudar a los responsables a presentar unas notificaciones de forma armonizada y conforme al RGPD.

6.7 Evaluaciones de impacto sobre la protección de datos

Los responsables deberán **realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) antes de iniciar los tratamientos** que puedan suponer **un alto riesgo** para los derechos y libertades de los **interesados**.

IMPORTANTE: Cuando el a**nálisis de riesgo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD revelen un alto riesgo** para los derechos o libertades de los interesados, **los responsables deberán realizar una EIPD sobre esos tratamientos**, y adoptar las medidas necesarias para adaptar el tratamiento a las exigencias del RGPD.

Si una **EIPD identifica un alto riesgo que no pueda mitigarse** por medios razonables (tecnología aplicable y costes) el responsable deberá **consultar a la autoridad** que podrá emitir recomendaciones al respecto e incluso prohibir la operación de tratamiento.



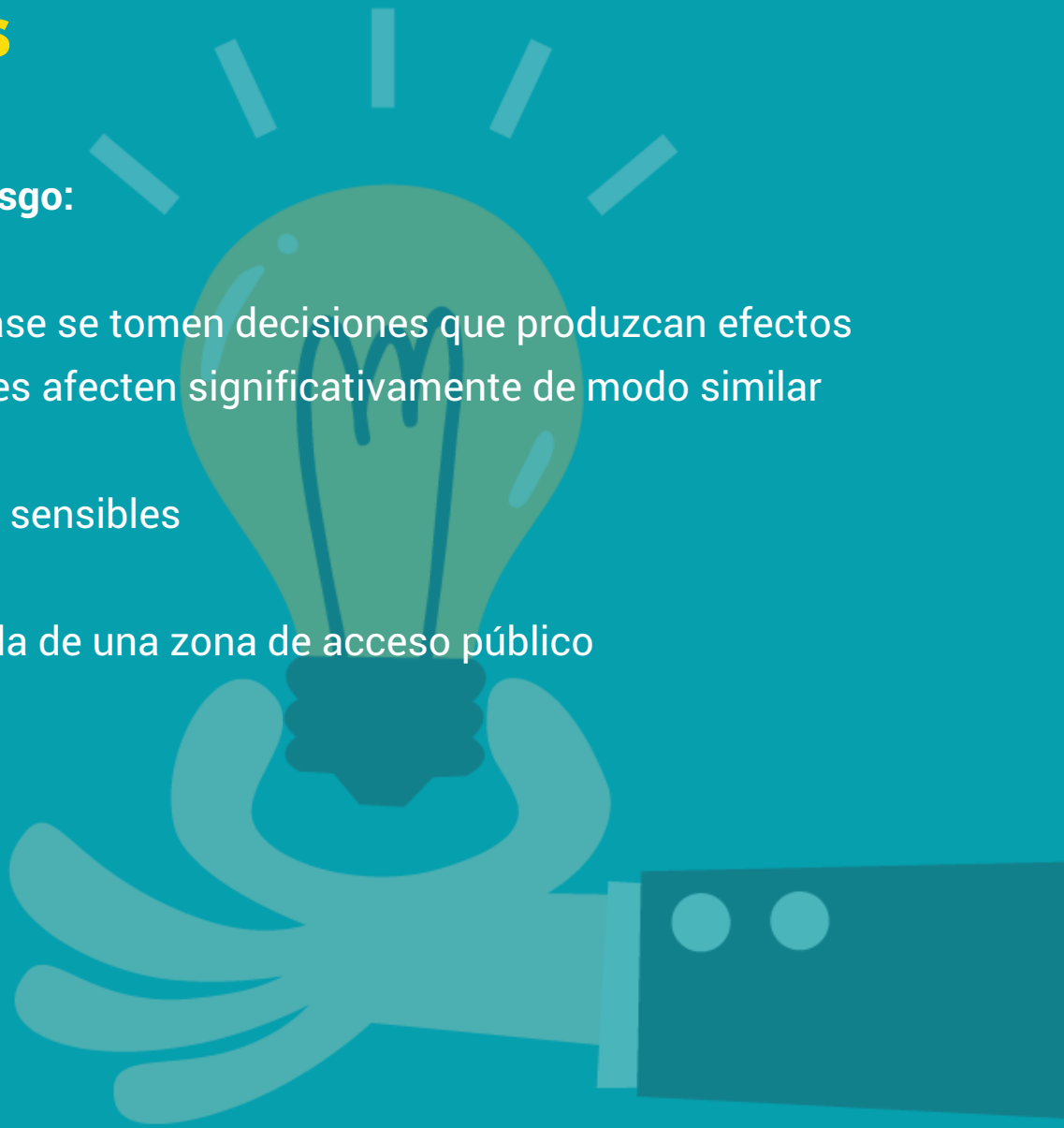
6.7 Evaluaciones de impacto sobre la protección de datos

Tratamientos que conllevan un alto riesgo:

• Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar

• Tratamientos a gran escala de datos sensibles

• Observación sistemática a gran escala de una zona de acceso público



LETSLAW

MITTUM

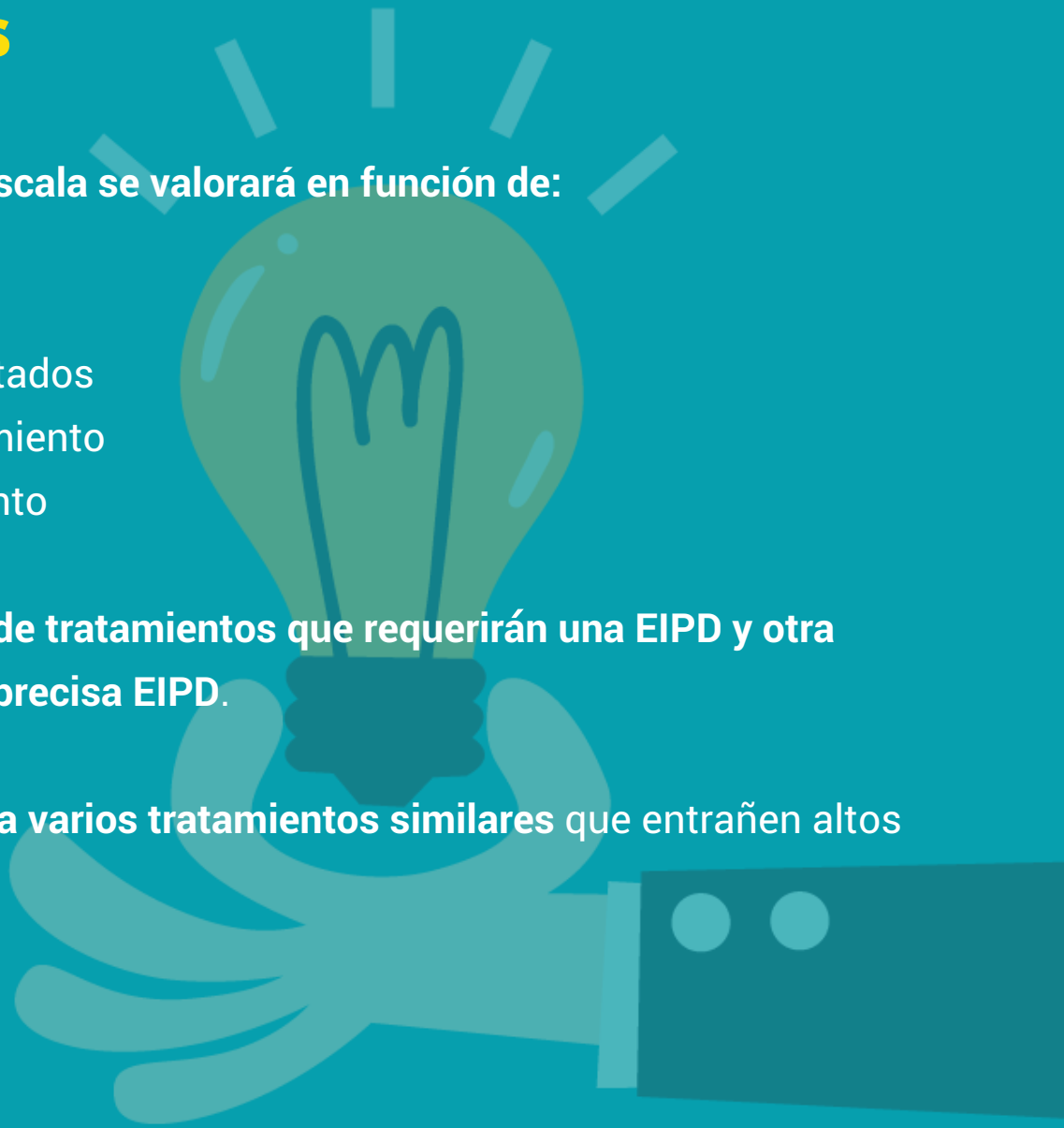
6.7 Evaluaciones de impacto sobre la protección de datos

La existencia de tratamientos a gran escala se valorará en función de:

- El número de interesados afectados
- El volumen y la variedad de datos tratados
- La duración o permanencia del tratamiento
- La extensión geográfica del tratamiento

La AEPD elaborará una **lista adicional de tratamientos que requerirán una EIPD y otra lista de tratamientos en los que no se precisa EIPD**.

Se permite realizar una única EIPD para varios tratamientos similares que entrañen altos riesgos también similares.



MITTUM

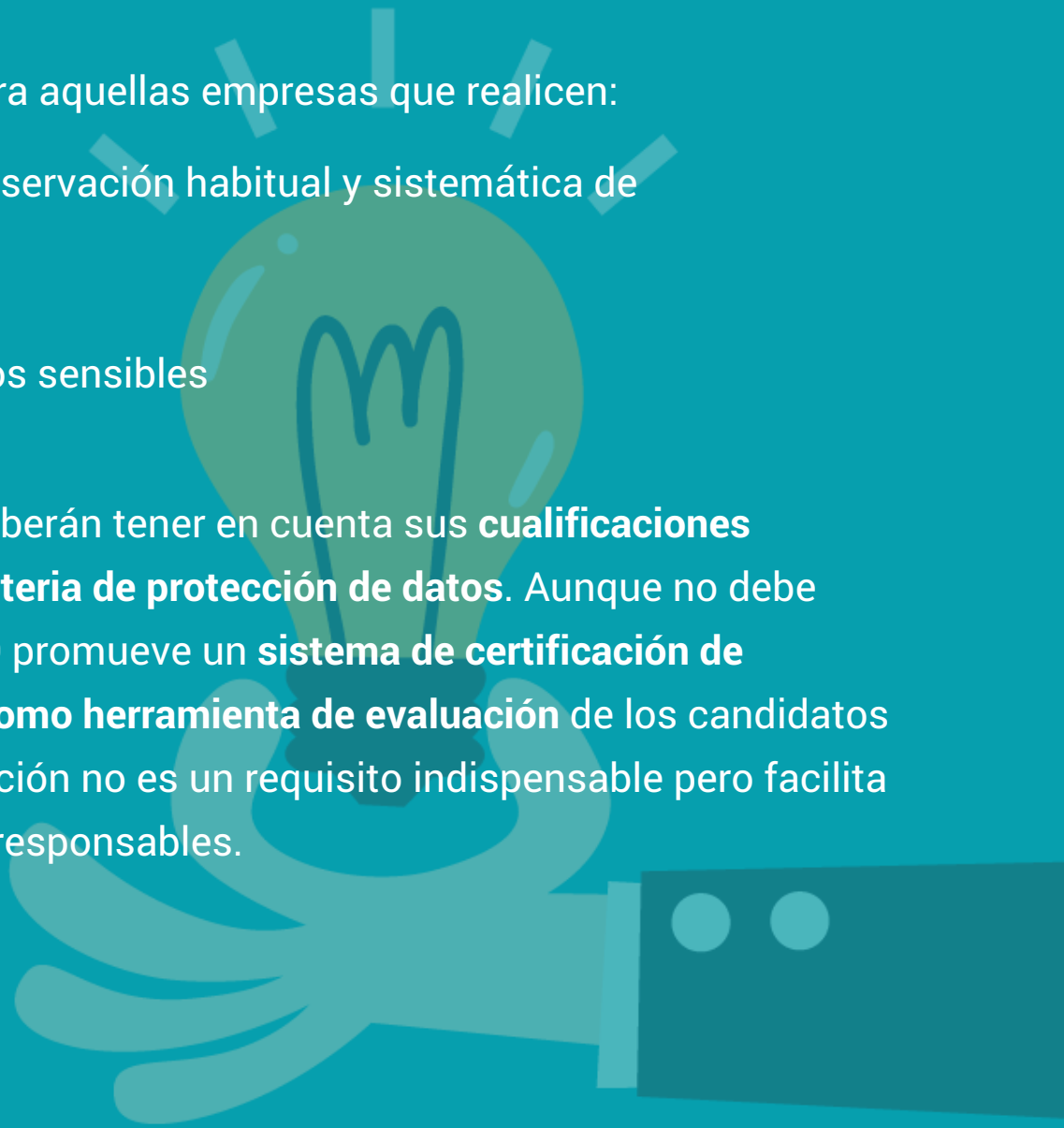
6.8 Delegado de Protección de Datos

Será **obligatorio contar con un DPO** para aquellas empresas que realicen:

- Tratamiento que requieran una observación habitual y sistemática de interesados a gran escala

- Tratamiento a gran escala de datos sensibles

Para nombrar un DPO, las empresas deberán tener en cuenta sus **cualificaciones profesionales y su conocimiento en materia de protección de datos**. Aunque no debe tener una titulación específica, la AEPD promueve un **sistema de certificación de profesionales de protección de datos como herramienta de evaluación** de los candidatos a ocupar el puesto de DPO. La certificación no es un requisito indispensable pero facilita la elección de DPO a los encargados y responsables.



6.8 Delegado de Protección de Datos

IMPORTANTE: La **designación del DPO y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades** de supervisión competentes.

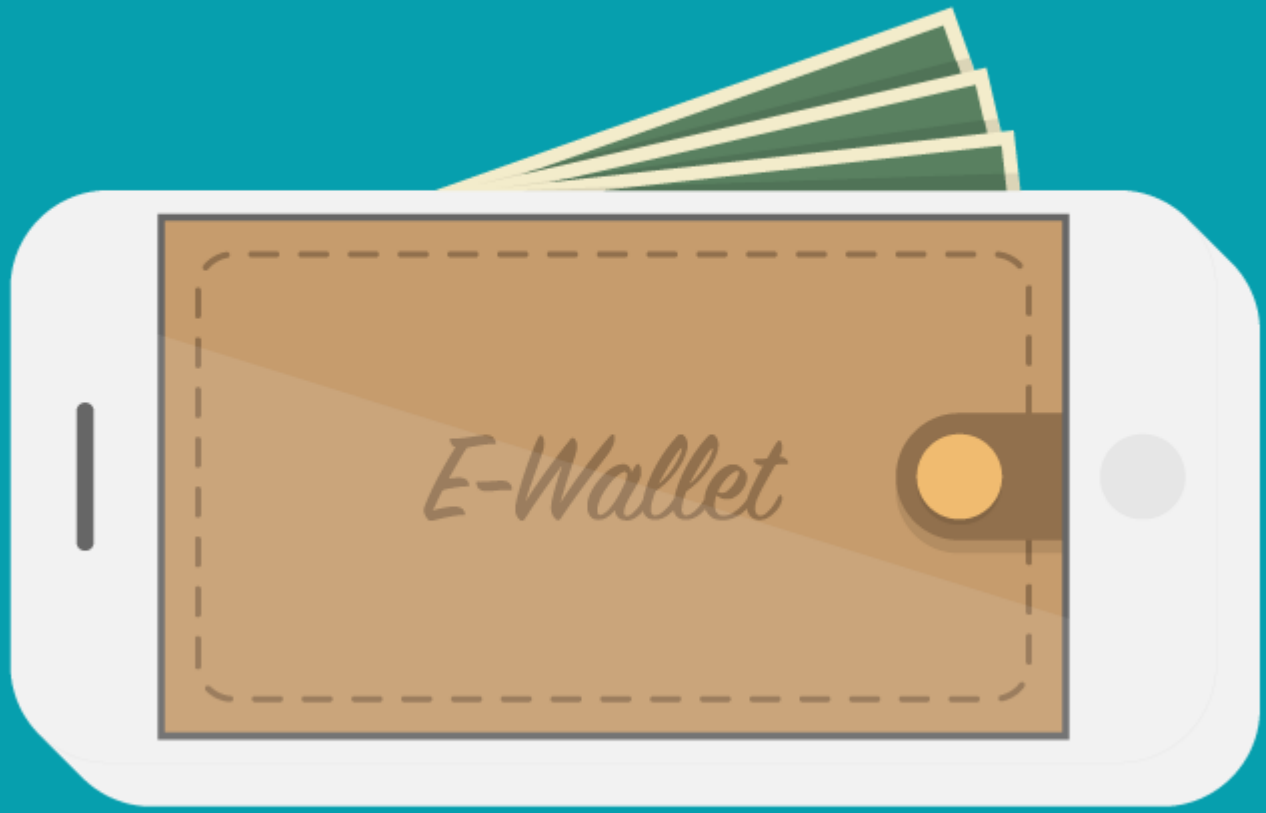
La posición del DPO deberá cumplir ciertos requisitos en las empresas:

- Autonomía en el ejercicio de sus funciones
- Se relacionará con el nivel superior de la dirección
- Obligación de que el responsable o el encargado le faciliten los recursos necesarios para desarrollar su actividad

Se permite **nombrar un solo DPO para un grupo empresarial**
Se permite que el DPO mantenga con responsables o encargados una **relación laboral o mediante un contrato de servicios**. Es decir, contratar como DPO a personas físicas o jurídicas ajenas a la organización. El RGPD prevé también el catálogo de funciones del DPO.

MITTUM

7. TRANSFERENCIAS INTERNACIONALES



LETSLAW

7. Transferencias Internacionales:

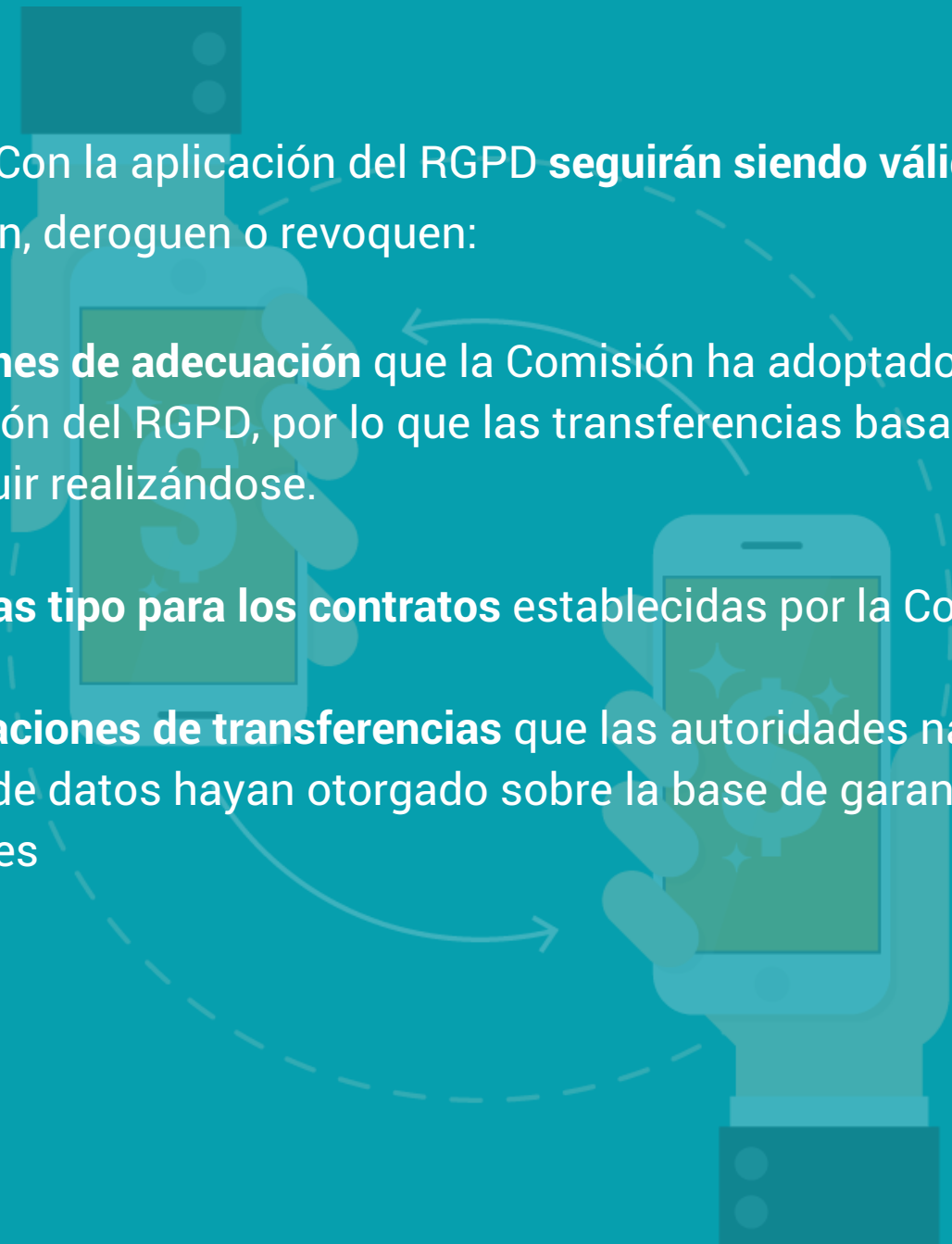
Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos con un **nivel de protección adecuado**
- Cuando el exportador haya ofrecido **garantías adecuadas** sobre la protección que los datos recibirán en su destino
- Excepciones por **razones de necesidad** vinculadas al propio interés interesado o al interés general.

7. Transferencias Internacionales:

IMPORTANTE: Con la aplicación del RGPD **seguirán siendo válidas** hasta que no se sustituyan, deroguen o revoquen:

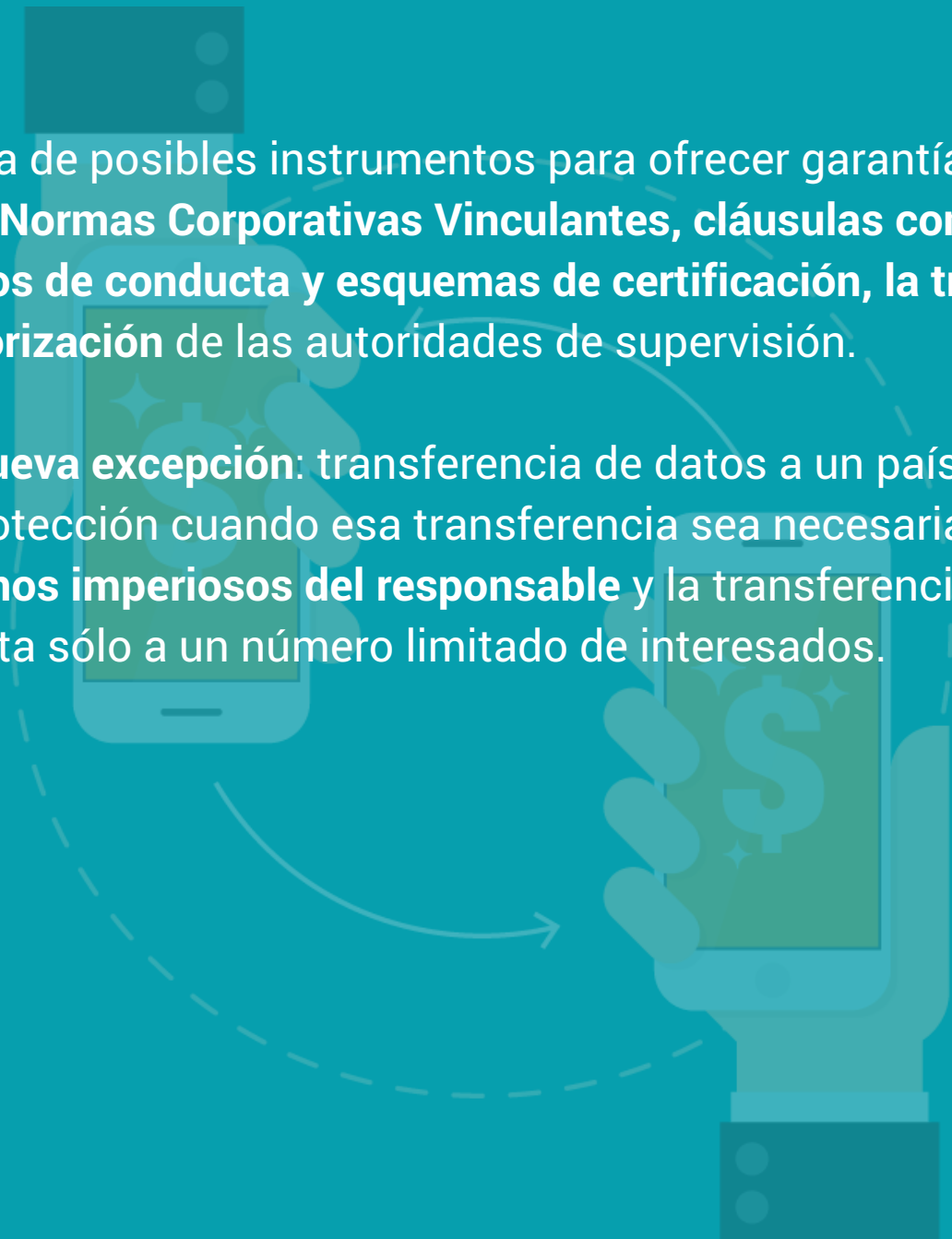
- **Las decisiones de adecuación** que la Comisión ha adoptado con anterioridad a la aplicación del RGPD, por lo que las transferencias basadas en ellas podrán seguir realizándose.
- Las c**láusulas tipo para los contratos** establecidas por la Comisión
- Las **autorizaciones de transferencias** que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales



7. Transferencias Internacionales:

Se amplía la lista de posibles instrumentos para ofrecer garantías: En concreto, en los casos de **Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización** de las autoridades de supervisión.

Se añade una **nueva excepción**: transferencia de datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para **satisfacer intereses legítimos imperiosos del responsable** y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados.



MITTUM

8. TRATAMIENTOS DE DATOS DE MENORES:

LETSLAW

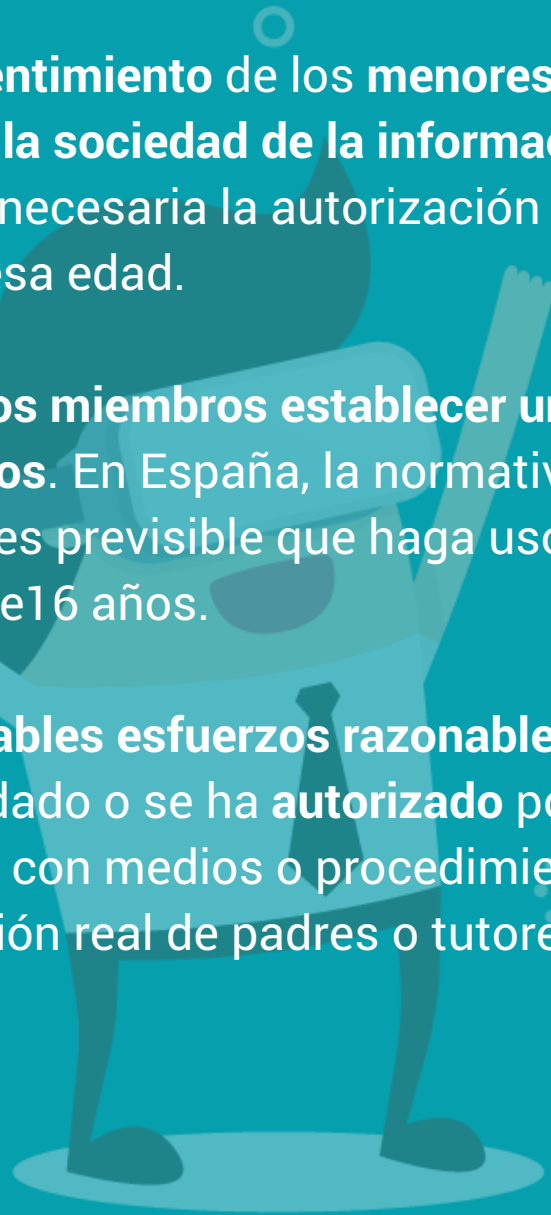
MITTUM

8. Tratamientos de Datos de Menores:

- La obtención del **consentimiento** de los **menores** en el ámbito de la **oferta directa de servicios de la sociedad de la información** solo será válida a partir de los **16 años**, siendo necesaria la autorización de los padres o tutores legales por debajo de esa edad.

- **Se permite a los estados miembros establecer una edad inferior**, siempre que **no sea menor de 13 años**. En España, la normativa nacional fija esta edad en los 14 años por lo que es previsible que haga uso de la facultad de establecer una edad inferior a la de16 años.

- Se **exige a los responsables esfuerzos razonables en la verificación** de que el **consentimiento** se ha dado o se ha **autorizado** por los padres o tutores del menor (deberán contar con medios o procedimientos razonables para establecer la intervención real de padres o tutores).



LETSLAW

¡GRACIAS!

WWW.MITTUM.COM

Contenidos elaborados por:

LETSLAW