Wolters Kluwer

When you have to be right

5 aspectos clave del RGPD para departamentos jurídicos

Afrontar los desafíos y entender tus obligaciones jurídicas bajo el nuevo Reglamento General de Protección de Datos (RGPD)

5 aspectos clave del RGPD para departamentos jurídicos

El Reglamento general de protección de datos europeo (en adelante, el RGPD) entrará en vigor el 25 de mayo de 2018, en sustitución de la actual Directiva de 1995 sobre protección de datos (Directiva 95/46/CE).

En virtud del RGPD, las empresas deberán hacer un esfuerzo considerablemente mayor para cumplir los nuevos requisitos de protección de datos con respecto a los datos personales. Ya no se trata solo de seguir las prácticas recomendadas a la hora de tratar datos privados y prevenir una filtración. Las regulaciones jurídicas sobre los derechos individuales, el requisito de mantener registros del tratamiento de datos y la necesidad de implementar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo representan retos totalmente nuevos para los departamentos jurídicos y los responsables de la protección de datos.

Las empresas que no cumplan la normativa pueden verse sometidas a multas de hasta **veinte millones de euros o el 4 % de sus ingresos globales**. Pero eso no es todo. Según otras leyes de protección de datos locales, que se aplican junto con el RGPD, también podrías tener que **hacer frente a sanciones criminales y administrativas, y/o reclamaciones por daños**, derivadas del incumplimiento o la vulneración de las leyes de tu jurisdicción. En Alemania, la Ley Federal de protección de datos prevé multas en caso de faltas administrativas o incluso penas de prisión en caso de delitos[1]. En el Código Penal de Francia se tipifican una serie de delitos por incumplimiento o vulneración de la legislación en materia de protección de datos

que pueden castigarse con **penas de prisión de cinco años y una sanción económica de trescientos mil euros en el caso de particulares** (en el caso de entidades jurídicas, el importe de esta sanción se multiplica por cinco)[2].

Para muchas empresas, la pregunta «¿Quién debería tener el RGPD?» puede que no obtenga respuestas demasiado claras. Los departamentos jurídicos internos desempeñan un papel importante a la hora de mitigar los riesgos legales para garantizar la implementación efectiva de un programa de cumplimiento de RGPD. Además, el departamento jurídico puede abanderar los esfuerzos y fomentar la colaboración con otros departamentos, como el informático, para que la infraestructura y los sistemas faciliten el cumplimiento de los nuevos requisitos derivados del RGPD. De hecho, según un informe de Legal Week Intelligence, casi el 50 % de los miembros del departamento jurídico afirma que su implicación en el tema de los riesgos cibernéticos se ha visto reforzada para incorporar la planificación de incidentes de seguridad cibernética y responder a esos ataques[3].

En este documento, haremos hincapié en los aspectos clave del RGPD que todos los departamentos jurídicos deben comprender. Eso incluye:

- demostrar un fundamento jurídico para el tratamiento de datos,
- mantener registros precisos,
- entender tus obligaciones si ocurre una filtración de datos,
- desarrollar un plan de mitigación de riesgos, y
- cómo la tecnología puede ayudarte con el cumplimiento normativo

Aspecto 1: Demostrar un fundamento jurídico para la recopilación y el tratamiento de datos personales.

Bajo el artículo 5(1) del RGPD, debes identificar un fundamento jurídico antes de procesar datos personales. El artículo 6 del RGPD establece una lista de todos los fundamentos jurídicos disponibles para el tratamiento de datos personales. Si no cuentas con un fundamento jurídico en virtud del artículo 6, el tratamiento de datos no es lícito para tu actividad. El tratamiento solo será lícito si al menos una de las bases jurídicas contempladas en el artículo 6(1)(a)-(f) se cumple. Si tomamos como ejemplo el artículo 6(1)(a) como base jurídica, necesitamos una combinación de propósito específico y el consentimiento explícito del usuario. De este modo, debes garantizar que el consentimiento para procesar datos para un propósito específico se solicite, obtenga,registre, controle y modifique según los requisitos del RGPD.

El consentimiento debe ser una indicación expresada con libertad, específica, fundamentada y sin ambigüedades de los deseos de la persona.

Al usar el consentimiento de la persona interesada como base del tratamiento lícito, se deben cumplir las siguientes condiciones:

- Cuando el tratamiento se basa en el consentimiento, el responsable del tratamiento debe poder demostrar que la persona interesada ha dado su consentimiento para procesar sus datos personales. El consentimiento se debe poder verificar, lo cual significa que el responsable del tratamiento debe poder proporcionar pruebas de dicho consentimiento. (Art. 7 RGPD)
- Las solicitudes de consentimiento deben ser claras y directas, separadas de otros términos y condiciones. Esto solo se puede conseguir si se separa claramente la solicitud de consentimiento del resto del texto (por ejemplo, usando impresión en negrita o incluyendo la sección de consentimiento en un recuadro independiente). (Art. 7 RGPD)
- Debe haber algún tipo de acción afirmativa clara o, en otras palabras, una aceptación. El consentimiento no puede deducirse a partir de la inactividad o de casillas ya marcadas.
- La persona interesada debe tener el derecho de retirar su consentimiento en cualquier momento. La revocación del consentimiento no afectará la legitimidad del tratamiento basado en el consentimiento antes de su revocación. Antes de dar su consentimiento, la persona interesada deberá ser informada sobre esa cuestión. Revocar el consentimiento deberá ser tan fácil como darlo en primera instancia.
- Las personas suelen tener más derechos cuando se depende del consentimiento para procesar sus datos. Estos derechos individuales (que están detallados en los artículos 12-23 del RGPD) incluyen el derecho de ser eliminado («el derecho al olvido»), el derecho a la portabilidad de datos, el derecho de oposición al tratamiento, a la elaboración de perfiles, etc.
- La persona interesada debe ser informada sobre cómo se usarán sus datos personales, así como de sus derechos individuales, incluyendo el derecho a revocar el consentimiento (o derecho a no participar) en cualquier momento (§ 51(3) párr. 3 de la Ley Federal de Protección de Datos alemana n.v.). Por ejemplo, en una política de privacidad clara y directa.
- Para categorías especiales de datos personales (como los datos que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas), el consentimiento debe hacer referencia explícita a estos datos (art. 9 del RGPD)
- De acuerdo con el principio de integridad y confidencialidad, los responsables del tratamiento deben adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado de los datos personales, y así ofrecer protección efectiva contra el tratamiento ilícito o no autorizado y contra pérdidas, destrucción o daños accidentales (ver art. 5(1)(f) del RGPD).

En los artículos 8-11, el RGPD también establece pautas adicionales para el tratamiento de categorías especiales de datos personales que son, por su naturaleza, especialmente confidenciales en relación con derechos y libertades fundamentales y exige una protección específica, ya que el contexto de su tratamiento podría originar riesgos considerables de los derechos y libertades fundamentales (en adelante, «datos confidenciales»). Por ejemplo, si estás recopilando datos personales de niños a efectos de marketing, también deberás entender qué método emplear para verificar la edad y obtener el consentimiento del padre, la madre o el tutor (art. 8 del RGPD). Además, a la hora de gestionar información sobre empleados, las empresas deben tener especial cuidado, porque hay muchas probabilidades de procesar datos confidenciales. También es oportuno señalar que algunos datos confidenciales pueden estar sujetos a requisitos adicionales de cada país.

Aspecto 2: Mantener documentación y registros precisos sobre qué datos procesas y cómo se usan

El RGPD establece requisitos generales en relación a la documentación y las pruebas de conformidad con la normativa. Los responsables del tratamiento deberán probar que su tratamiento de datos cumple con los requisitos del RGPD y proporcionar registros de estas actividades, según lo dispuesto en el artículo 30 del RGPD.

Si tu empresa cuenta con 250 empleados o más, debes mantener registros internos adicionales de tus actividades de tratamiento. Sin embargo, esta obligación también se aplica a empresas más pequeñas si:

1. es probable que el tratamiento suponga un riesgo en relación con los derechos de los empleados afectados (p. ej. calificación,supervisión exhaustiva, alto riesgo por el acceso o la publicación no autorizados, el uso de nuevas tecnologías),
2. el tratamiento no es puntual; o
3. el tratamiento incluye categorías especiales de datos:
    a. en virtud del contenido del artículo 9 (1) (p. ej. datos de salud, datos biométricos, datos relacionados con las convicciones políticas o filosóficas); o
    b. datos personales relacionados con delitos y condenas penales mencionados en el artículo 10.

Los registros de las actividades de tratamiento deben estar por escrito o en formato electrónico, y deben ponerse a disposición de las autoridades supervisoras si así lo solicitan (ver Apéndice B para un ejemplo de los requisitos del contenido). Si los requisitos no se cumplen, podrá aplicarse una multa administrativa de hasta diez millones de euros o hasta el 2 % de los ingresos globales anuales (art. 83(4) del RGPD).

También es importante recordar que, aunque tu empresa no esté obligada a mantener registros de tratamiento de datos,en caso de filtración, deberás determinar los tratamientos de datos implicados para entender las consecuencias de la brecha y estudiar cómo mitigar riesgos en el futuro. Cuantos más registros realices, más sencillo te resultará tomar las mejores decisiones sobre la protección de dados.

Es posible que debas proporcionar estos registros a las autoridades supervisoras competentes a efectos de realizar una investigación, de modo que es crucial que tengas a mano la siguiente información:

- directrices sobre seguridad informática, cumplimiento y protección de datos;
- responsabilidades y manual de protección de datos;
- declaraciones en materia de protección de datos de todos los empleados encargados del tratamiento de datos personales;
- esquemas de tratamiento relativos a todos los procesos automatizados pertinentes (tratamiento de datos electrónicos);
- pruebas permanentes de declaraciones de consentimiento sobre la recogida de datos personales, en particular para marketing directo y comercio electrónico

Una de las preocupaciones de los departamentos jurídicos es perderse en las complejidades del RGPD, así que es importante recordar que el RGPD concierne los derechos de propiedad vinculados a la información y, en consecuencia, las empresas deben decidir dónde se procesarán y almacenarán los distintos tipos de datos, incluyendo diferentes categorías de información personal identificable (PII, por sus siglas en inglés). Lo cierto es que en la actualidad las empresas cuentan con múltiples bases de datos y CRM, pero no tienen las herramientas necesarias para extraer los datos personales relevantes con el objetivo de auditar adecuadamente o llevar a cabo verificaciones de diligencia debida.

Mantener un registro o «mapa» que clarifique dónde se encuentra cada tipo de datos y los parámetros para tratarlos es tu obligación, y te ayudará a mitigar el riesgo de filtraciones de datos. Por norma general, los datos personales solo deberían almacenarse donde indique tu política corporativa.

Aspecto 3: Entender tus obligaciones si ocurre una filtración de datos

Una filtración de datos, según el RGPD, es una filtración en la seguridad que lleva a la destrucción, pérdida, alteración o divulgación no autorizada (o acceso) de datos personales. Las obligaciones de informar y notificar en caso de que se haya producido una brecha de seguridad que afecte tus datos están establecidas en el RGPD,en los artículos 33 y 34.

Cuando se produce una filtración de datos personales, el responsable del tratamiento debe notificarlo a las autoridades competentes sin demora indebida, como máximo 72 horas después de tener conocimiento de la filtración. Esto puede estar sujeto a requisitos adicionales, según el país.

Sin embargo, no hay obligación de informar sobre si es poco probable que la brecha suponga un riesgo para los derechos y las libertades de las personas naturales, o si la información no puede identificarse. Analizar estos aspectos y determinar si existe la obligación de informar en un determinado caso no siempre será sencillo.

La notificación a la autoridad de control competente deberá contener, como mínimo, la información siguiente:

- descripción de la naturaleza de la filtración de datos personales, incluyendo, siempre que sea posible, las categorías y el número aproximado de personas afectadas y las categorías y el número aproximado de registros de datos personales afectados;
- el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto que pueda proporcionar más información;
- descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;
- descripción de las medidas tomadas o sugeridas por el responsable del tratamiento para abordar la filtración de datos personales, incluyendo, cuando corresponda, medidas para mitigar sus posibles efectos negativos.

Si fuera necesario, el responsable del tratamiento podrá facilitar la información exigida jurídicamente de manera gradual, cuando no sea posible facilitarla en un plazo de 72 horas. Ahora bien, el departamento jurídico deberá tener en cuenta los distintos períodos de notificación de cada jurisdicción. Por ejemplo, en Francia la CNIL requiere una primera notificación durante las primeras 24 horas, mientras que la Comisión de Protección de Datos belga requiere una primera notificación durante las primeras 48 horas. Si tienes entidades en distintas jurisdicciones, debes responder de forma apropiada para cumplir con los requisitos de cada país; de lo contrario, corres el riesgo de recibir sanciones.

El responsable del tratamiento está asimismo sujeto a una amplia obligación de documentación con arreglo a lo dispuesto en el artículo 30(5) del RGPD.

El procesador también debe informar sobre una filtración de datos personales al responsable del tratamiento después de tener conocimiento de dicha filtración, sin demora (art. 30(2) del RGPD).

De la misma manera, el responsable del tratamiento deberá comunicar la violación de la seguridad de los datos personales a la persona interesada sin dilación indebida y en un «lenguaje claro y sencillo», con arreglo al artículo 34 del RGPD.

No es necesario notificar a la persona interesada en los casos siguientes:

- si el responsable del tratamiento ha implementado medidas de seguridad técnicas y organizativas para que los datos personales sean ininteligibles para cualquier persona que no tenga autorización para acceder a ellos (en particular, el cifrado);
- si el responsable del tratamiento ha tomado medidas posteriores que garanticen que ya no es probable que los derechos y las libertades de las personas interesadas afectadas corran un alto riesgo;
- si puede suponer un «esfuerzo desproporcionado»; aunque, en este caso debe haber una comunicación pública o una medida similar, mediante la cual las personas interesadas reciban la información de forma igualmente eficaz.

La autoridad supervisora puede llevar a cabo una evaluación independiente y obligar al responsable del tratamiento a informar a las personas interesadas sobre la filtración, aunque sea bastante tiempo más tarde.

Aspecto 4: Desarrollar un marco de mitigación de riesgos para minimizar tus riesgos de responsabilidad

Es necesario un sistema de datos integrados apropiado e implementado para evitar o minimizar los riesgos, ya que podrían poner en peligro la propia existencia de la empresa.

Esta podría ser una lista de medidas para conseguir dicho objetivo y minimizar los riesgos de responsabilidad:

1. Análisis de los requisitos legales, técnicos y organizativos que la empresa debe cumplir, integrando a la dirección, el departamento jurídico, el departamento informático y el delegado de protección de datos, con el apoyo de asesores externos si corresponde.
2. Establecimiento de políticas, regulaciones y directrices obligatorias sobre protección de datos y seguridad informática (o revisión de las ya existentes para tener en cuenta el RGPD), además de la comunicación a todos los empleados y, en particular, a los departamentos responsables del tratamiento de datos electrónicos.
3. Lanzamiento de una «página web de cumplimiento» y formación periódica para los empleados, que debe incluir cómo gestionar correctamente los datos personales.
4. Elaboración y publicación de un plan de acción que incluya los requisitos de una Evaluación del Impacto sobre la Protección de Datos, en caso de que sea necesaria.
5. Refuerzo de la función del delegado de protección de datos dentro de la empresa.
6. Integración del comité de empresa en el tratamiento de los datos personales de los empleados, y como acuerdos colectivos relevantes y concluyentes.
7. Uso de métodos y tecnologías apropiados para una protección de datos integrada y garantizar una seguridad de datos adecuada.
8. Aplicación de ajustes predeterminados que contribuyan a la protección de datos en sistemas informáticos, donde las aplicaciones recopilan o procesan datos personales a través de medios automatizados.
9. Uso de soluciones tecnológicas jurídicas adecuadas para gestionar la información con eficiencia, almacenar de forma permanente documentos legales, documentar procesos de relevancia jurídica y comunicar estos aspectos a un organismo central.
10. Auditorías regulares para evaluar el nivel actual de protección de datos en la empresa y comprobar si es legítimo seguir almacenando datos personales.

Más allá de la responsabilidad corporativa, sin embargo, también hemos observado un aumento constante de acciones dirigidas de forma individual a directores y delegados por parte de reguladores y accionistas. Tal y como hemos mencionado anteriormente, según las leyes locales de protección de datos que se aplican en paralelo al RGPD, también podrías enfrentarte a sanciones criminales y administrativas y/o reclamaciones por daños. El fundamento principal son alegaciones que afirman que los directores y los delegados incumplieron distintos deberes fiduciarios, como los de diligencia y lealtad.

En el marco de una filtración de datos, las investigaciones normalmente giran en torno al conocimiento de los directores sobre sus actividades de tratamiento de datos y los riesgos que implicaban, y las acciones que emprendieron para prevenir estos riesgos. Por este motivo, además de tomar acciones en toda la empresa para protegerla de responsabilidad, los directores y los delegados deben tomar medidas para minimizar el riesgo de incurrir en responsabilidad personal.

Aspecto 5: Cómo puede ayudar la tecnología jurídica

Las obligaciones de los responsables del tratamiento y los procesadores de datos han aumentado en comparación con la Directiva de Protección de Datos de 1995, lo cual ha derivado en un riesgo mayor para las empresas, que deberán hacer frente a una cantidad cada vez mayor de demandas por parte de personas interesadas, a la vez que tendrán que revisar sus políticas de responsabilidad. Por suerte, la tecnología puede ayudarte a controlar el tratamiento de datos y las filtraciones para evitar sanciones. La naturaleza y la cantidad de estos tratamientos de datos imposibilita el control manual de datos personales.

La protección estratégica de datos y la tecnología jurídica van de la mano. Las herramientas inteligentes ofrecen soporte a la hora de analizar, optimizar y documentar todos los procesos relevantes de protección de datos. A continuación, se incluyen algunas de las ventajas y posibles aplicaciones de estas tecnologías especializadas:

- Almacenamiento de datos central y un análisis de datos más sencillo, rápido y fiable en tiempo real.
- Acceso, en cualquier momento, a todos los contratos y documentos jurídicos, además de la información definitiva sobre los procesos y las decisiones relevantes de acuerdo con la ley de protección de datos.
- Archivado de documentación jurídica importante, por ejemplo, acuerdos de confidencialidad, acuerdos con terceros en relación con el tratamiento de los datos o declaraciones de protección de datos de empleados.
- Gestión de un directorio central de procedimientos o una visión general del tratamiento, incluyendo los sistemas de procesadores de datos autorizados.
- Panel de gestión de riesgos que permita hacer seguimiento, independientemente de la ubicación, de actividades relevantes de tratamiento de datos personales, riesgos elevados y (contra-)medidas presentadas en tiempo real.
- Gestión central de los acuerdos con proveedores de servicios sobre tratamiento de datos, además de declaraciones de protección de datos de empleados, incluyendo recordatorios automatizados sobre documentación pendiente.
- Documentación fluida y adecuada en caso de auditoría de las responsabilidades y procesos en materia de tratamiento de datos electrónicos.
- Archivo de políticas y almacenamiento de listas de medidas, instrucciones, responsabilidades e información de contacto.
- Visión general del estado actual de las medidas formativas completadas, en curso y planificadas.
- Panel de tareas y correos electrónicos automáticos para recordar elementos pendientes destacados.
- Salas de datos protegidas para proyectos y datos sensibles.
- Gestión de acceso flexible para reducir al mínimo el número de personas que puede acceder a datos sensibles.
- Archivado de documentos contractuales que se han comprobado de conformidad con la ley de protección de datos.
- Generación automática de contratos, incluidos los anexos pertinentes a los efectos de la ley de protección de datos (por ejemplo, para obtener el consentimiento necesario para el tratamiento de los datos).

Ante los riesgos significativamente mayores de responsabilidad personal y la amenaza de multas draconianas, piensa que el uso de tecnologías modernas te permitirá trabajar de forma más eficiente y segura. Si no cuentas con la tecnología adecuada para cubrir tus necesidades, es hora de implementar una solución cuanto antes. Además,podrás externalizar al menos algunos de los riesgos de responsabilidad del ámbito de la protección y la seguridad de datos a proveedores de servicios externos.

Toma medidas a partir de estas preguntas de seguimiento:

1. ¿Sabes qué fundamento jurídico tienes para recopilar y procesar datos personales?
2. ¿La elaboración de perfiles u otros tratamientos están basados en el consentimiento explícito?
3. ¿Cuentas con una política de privacidad que cumpla plenamente con el RGPD?
4. ¿El manual y los contratos de tus empleados están actualizados de acuerdo con la normativa del RGPD?
5. ¿Sabes quién almacena tus datos y si dicha empresa actúa de acuerdo con el RGPD?
6. ¿Guardas los datos durante el período de tiempo correcto?
7. ¿Entiendes plenamente la gestión de los registros de tu empresa?
8. ¿Puedes restringir el tratamiento de la totalidad o parte de los datos de una persona interesada?
9. ¿Sabes qué debes hacer en caso de filtración de datos?
10. ¿Los sistemas que gestionan tus datos son seguros?

Gestionar información jurídica con Legisway

Como asesor jurídico, desempeñas un papel importante en el proceso de protección de datos de tu empresa. Debes poder gestionar la información jurídica de tu empresa para minimizar los riesgos, tanto si lo haces solo como si lo haces en colaboración con los delegados de protección de datos y/o cumplimiento normativo. Con **Legisway**, es fácil trabajar para que tu información jurídica cumpla con los requisitos del RGPD, garantizar que toda la empresa usa la versión más actualizada de las plantillas, registrar las actividades de tratamiento de datos y las filtraciones para evitar sanciones y reclamaciones.

Con **Legisway**, puedes:

- Auditar la solidez jurídica de la información de tu empresa. Revisar y adaptar el tratamiento de tus datos y acuerdos a los requisitos del RGPD mediante la creación de informes y el almacenamiento de tus plantillas en una única base de datos jurídica centralizada.
- Revisa y vuelve a redactar tus contratos y documentos jurídicos para garantizar su conformidad con el RGPD. Guarda tus plantillas en una única ubicación para poder crear fácilmente acuerdos de tratamiento de datos y nuevos términos y condiciones, a la vez que creas y exportas informes de actividad de tratamiento, informes de filtraciones de datos, etc. que cumplan con los principios del RGPD.
- Almacena y comparte tus plantillas y documentos jurídicos actualizados para cumplir con las nuevas obligaciones contractuales requeridas por el RGPD.
- Prepárate para las brechas de seguridad de datos, registra eventos y acciones jurídicas relacionadas para cumplir con la normativa. Registra tratamientos de datos, controla e informa sobre filtraciones de datos, delega las tareas y los plazos de acuerdo con los períodos de preaviso y más.

Con **Legisway**, puedes empezar poco a poco con una herramienta segura basada en la nube más potente que los discos duros compartidos, hojas de cálculo o herramientas genéricas, y más fácil de escalar que las aplicaciones independientes del RGPD.

Más información en Legisway.es

Apéndice A – Glosario

RGPD: Regulación (UE) 2016/679 del Parlamento europeo y el Consejo del 27 de abril de 2016 sobre la protección de personas físicas en relación con el tratamiento de datos personales y el libre movimiento de estos datos y la derogación de la directiva 95/46/EC (Reglamento General de Protección de Datos).

Datos personales: hace referencia a cualquier información relacionada con una persona física identificada o identificable.

Tratamiento: cualquier operación que consista en recopilar, registrar, organizar, almacenar, adaptar/modificar, recuperar, poner a disposición, combinar o cualquier otra acción en relación con los datos, incluyendo su eliminación y destrucción.

Responsable del tratamiento: cualquier persona física o jurídica, autoridad pública, agencia u organización que, de forma individual o en colaboración con otros, determina el propósito y los medios de tratamiento de datos personales.

Procesador: cualquier persona física o jurídica, autoridad pública, agencia u organización que procesa datos personales en nombre del responsable del tratamiento.

Datos personales confidenciales: datos personales, que revelan el origen racial o étnico, las opiniones políticas, la religión o las creencias, la afiliación a una organización sindical, la salud física o mental, o la vida sexual. El RGPD añade datos genéticos.

Elaboración de perfiles: cualquier tratamiento automatizado realizado para evaluar determinados aspectos personales, en particular para fines de análisis, predicción o uso selectivo.

Seudónimo: un tratamiento de tal naturaleza que los datos personales ya no pueden atribuirse a una persona interesada específica sin el uso de información adicional.

Autoridad de protección de datos (APD): cada estado miembro designa una o más autoridades para que implementen y apliquen las leyes de protección de datos en ese estado miembro.

Filtración de datos: cualquier filtración accidental en la seguridad que lleva a la destrucción, pérdida, alteración, divulgación no autorizada, o acceso, de datos personales.

Evaluaciones del impacto sobre la protección de datos: el artículo 35 del RGPD introduce un nuevo instrumento; la evaluación del impacto sobre la protección de datos (EIPD). Una EIPD sirve para identificar y evaluar los riesgos. En general, una EIPD siempre debería llevarse a cabo cuando sea probable que un tipo de tratamiento, en particular aquellos que usan nuevas tecnologías, conlleve un alto riesgo para los derechos y las libertades de las personas físicas a causa de la naturaleza, el alcance, el contexto y los propósitos del tratamiento. A la hora de implementar una evaluación del impacto sobre la protección de datos, también se debe buscar asesoramiento por parte del responsable de la protección de datos (si se ha designado dicho responsable) (artículo 35(2) del RGPD).

Responsable de la protección de datos: un responsable de la protección de datos (DPO, por sus siglas en inglés) es un puesto de liderazgo de seguridad empresarial requerido por el Reglamento General de Protección de Datos (RGPD). Los responsables de la protección de datos se encargan de supervisar la estrategia y la implementación de la protección de datos para garantizar el cumplimiento de los requisitos del RGPD. El artículo 37 define cuándo es necesario un DPO; el artículo 38 del RGPD define el puesto de los responsables de la protección de datos; mientras que el artículo 39 especifica cuáles son sus tareas.

Apéndice B

Ejemplo de los requisitos de contenido de los registros de tratamiento de datos

Nombre y detalles de contacto del:

- Responsable del tratamiento
- Representante del responsable del tratamiento (propietario, dirección, jefe de información),
- Representante de la UE, si el responsable del tratamiento no está establecido en la UE,
- Delegado de protección de datos

Debe proporcionarse información técnica y organizativa obtenida por procedimiento cruzado:

- Descripción de las medidas técnicas y organizativas para proteger los datos personales, en virtud del artículo 32 (1) del RGPD:
  1. la seudonimización y el cifrado de datos personales;
  2. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuadas de los servicios y sistemas de tratamiento;
  3. la capacidad de restablecer la disponibilidad y el acceso a datos personales de manera oportuna en caso de que ocurra un incidente técnico o físico;
  4. un proceso para evaluar y probar de forma regular la efectividad de las medidas técnicas y organizativas, para garantizar la seguridad del tratamiento
- A la hora de evaluar el nivel adecuado de seguridad se tendrá en cuenta, sobre todo, los riesgos que supone el tratamiento, en particular derivados de la destrucción accidental o ilegal, la pérdida, la alteración, la divulgación no autorizada o el acceso a datos personales transmitidos, almacenados o procesados de otra forma (art. 32(2)).
- Qué elementos pueden usarse para demostrar el cumplimiento de los requisitos establecidos en el art. 32 (1) y la conformidad con un código de conducta aprobado mencionado en el art. 40 de un mecanismo de certificación aprobado, tal y como se menciona en el art. 42.
- concepto de supresión

Debe proporcionarse la información especificada en las operaciones separadas de tratamiento de datos:

- nombre de la operación de tratamiento de datos
- fines del tratamiento
- categorías de personas interesadas
- categorías de datos personales
- categorías de destinatarios a quienes se han revelado o se revelarán los datos personales (internos y externos)
- categorías de destinatarios en otros países u organizaciones internacionales
  1. destinatario
  2. tercer país u organización
  3. suficientes garantías para la protección de los datos y los derechos de las personas interesadas en el tercer país u organización internacional
- límites de tiempo para el período de eliminación de datos
- si corresponde: medidas especiales de protección de datos.
- En caso de tratamientos de datos que hayan sido encargados, además de la información general de los responsables también debe proporcionarse información sobre el procesador de datos encargado.

Cada procesador (y su representante) debe llevar un registro de las actividades de tratamiento realizadas en nombre del responsable del tratamiento, que incluya:

- el nombre y los detalles de contacto del responsable/procesador y cualquier representante/DPO;
- las categorías de las actividades de tratamiento realizadas;
- información sobre transferencias internacionales de datos; y
- una descripción general de las medidas de seguridad implementadas respecto al tratamiento de datos

Para más información, visita
Legisway.es

O llama al
91 6020182 /// 902 250 500

1. «Una guía comparativa de las sanciones en materia de seguridad de datos impuestas en más de diez jurisdicciones», Lexology
2. Ditto
3. Los directores jurídicos estudian informes ampliados de seguridad cibernética, y las empresas sitúan la responsabilidad en los servicios jurídicos para abordar las amenazas tecnológicas, Law.com
4. La obligación de diligencia normalmente obliga a los directores a actuar de forma fundamentada, de buena fe y con la honesta convicción de que la acción beneficiaba plenamente a la empresa. La obligación de lealtad, por otro lado, les obliga a desarrollar y realizar un seguimiento de los controles y los sistemas de notificación para garantizar que están debidamente informados de cualquier riesgo que requiera su atención.

Wolters Kluwer

When you have to be right