GUÍA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

JONES DAY® | One Firm Worldwide℠

ÍNDICE DE CONTENIDO

Introducción 3

Ámbito de aplicación 4

Bases legales para el tratamiento de datos 5

Derechos de los interesados 6

Mecanismos de gobierno y rendición de cuentas 8

Obligaciones y contratos de encargado de tratamiento 9

Seguridad de los datos personales y notificación de violación de la seguridad de los datos personales 10

Códigos de Conducta y Certificaciones 11

Transferencias internacionales de datos 12

Supervisión por las Autoridades de Protección de Datos 13

Recursos, Responsabilidades y Sanciones 14

Glosario 15

Información de contacto 17

INTRODUCCIÓN

En Mayo de 2016 la Unión Europea ("**UE**") publicó el Reglamento General de Protección de Datos de la Unión Europea ("**RGPD**"). Este instrumento legislativo representa el cambio más significativo en la legislación de protección de datos de la UE desde el año 1995. El RGPD se aplicará a todos los Estados miembros de la UE a partir del 25 de mayo de 2018.

El RGPD es un instrumento legal de gran alcance que tendrá un impacto significativo en todas las compañías implicadas en el tratamiento de datos personales, incluyendo a muchas entidades localizadas fuera de la UE. Se aumentarán las sanciones en caso de incumplimiento, con multas de hasta 20 millones de euros o el 4 por ciento del volumen de negocios anual a nivel global. Además, las autoridades de control dispondrán de amplios poderes.

Las compañías deben revisar el RGPD y empezar a prepararse para el cumplimiento de este nuevo marco legal de protección de datos en la UE.

Esta guía, proporciona un breve resumen de las nuevas reglas impuestas por el RGPD y los cambios clave contenidos en el mismo. La guía también incluye un breve glosario de términos utilizados en el RGPD, y, en cada sección, se establece una breve lista de tareas a realizar para su cumplimiento. La guía será desarrollada en breve por orientaciones adicionales, informes y listas de verificación sobre el RGPD.

Esperamos que esta guía constituya una herramienta útil. Por favor, póngase en contacto con cualquiera de los abogados que figuran en la página 17 si desea recibir información adicional.

ÁMBITO DE APLICACIÓN

ARTÍCULOS 2-3

Visión general

El RGPD se aplica al tratamiento de datos personales automatizados o que forman parte de un fichero o sistema. El ámbito subjetivo y territorial de aplicación del RGPD es más amplio que el de la Directiva Europea de Protección de Datos ("**Directiva**").

Aplicación

- El RGPD se aplica a ambos, a los responsables y a los encargados de tratamiento.
- El RGPD no se aplica a un número limitado de áreas, tales como el tratamiento de actividades exclusivamente personales o domésticas.

Ámbito territorial

El RGPD se aplica al tratamiento:

- En el contexto de un establecimiento en la UE; y
- Por un responsable o encargado de tratamiento *no* establecido en la UE de datos de los interesados en la UE que se refieran a:
  - *La oferta de bienes o servicios a dichos interesados; o*
  - *El control del comportamiento de los interesados.*

Siguientes pasos

- ✓ Identificar los tratamientos relevantes de datos personales.
- ✓ Confirmar que establecimientos de la UE tratan datos personales y cuáles de los tratamientos se refieren a situaciones en las que los bienes o servicios son ofrecidos en la UE o al control de los interesados en la UE.
- ✓ Evaluar si el tratamiento se realiza como un responsable o como un encargado.
- ✓ Determinar si un representante en la UE es necesario.

BASES LEGALES PARA EL TRATAMIENTO DE DATOS

ARTÍCULOS 6,7 Y 8

Visión general

Las bases legales para el tratamiento de datos personales, bajo el RGPD, son prácticamente las mismas que las de la Directiva. Sin embargo, el RGPD establece nuevas restricciones para el consentimiento, para el tratamiento basado en el interés legítimo y para el tratamiento para finalidades adicionales.

Bases legales para el tratamiento de datos personales

Las bases legales para el tratamiento de datos personales bajo el RGPD son:

- Cuando el interesado dé su consentimiento; y
- Cuando el tratamiento sea necesario:
  - Para la ejecución o la negociación de un contrato con el interesado;
  - Para cumplir con una obligación legal;
  - Para proteger los intereses vitales del interesado o de otra persona cuando el interesado sea incapaz de dar su consentimiento;
  - Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poder público; y
  - Para la satisfacción de los intereses legítimos (pero sujetos a los derechos y libertades fundamentales).

Nuevas restricciones sobre el consentimiento, el tratamiento basado en "intereses legítimos" y, el tratamiento para finalidades adicionales

- Para el tratamiento basado en el consentimiento, el responsable debe ser capaz de demostrar que el consentimiento ha sido dado libremente por el interesado, y la solicitud de consentimiento debe ser claramente perceptible.
- El RGPD clarifica cuando el "interés legítimo" puede ser utilizado como base para el tratamiento (por ejemplo, el marketing directo, la prevención del fraude, el intercambio de datos personales dentro de un grupo de empresas para la administración interna, seguridad de la red y la seguridad de la información) y requiere que el responsable informe al interesado cuando el tratamiento se base en el interés legítimo.
- El RGPD proporciona una lista de criterios que deben considerarse para determinar si el tratamiento de datos para una nueva finalidad es compatible con la finalidad original para la que se recogieron los datos.

Siguientes pasos

- ✓ Evaluar las bases legales utilizadas para los tratamientos actuales y revisar si siguen siendo válidas bajo el RGPD.
- ✓ Asegurar que el consentimiento ha sido dado de acuerdo con los nuevos requisitos y que el responsable lo puede demostrar.
- ✓ Cuando el tratamiento se base en el "interés legítimo", garantizar que:
  - El equilibrio del interés frente a los derechos de los interesados están documentados; y
  - Cuando un responsable se base en el interés legítimo como base para el tratamiento, este hecho sea incluido en la información proporcionada a los interesados.
- ✓ Garantizar que los procesos internos de gestión documentan los motivos que sustentan la decisión de utilizar los datos para finalidades adicionales de tratamiento.

DERECHOS DE LOS INTERESADOS

ARTÍCULOS 12-17, 19-20 Y 21.

Visión general

Los responsables de tratamiento deben ser más transparentes con los interesados, los cuales han visto incrementados los derechos de acceso a sus datos y se les ha reconocido importantes y nuevos derechos para exigir la rectificación o supresión de sus datos personales y para restringir el tratamiento adicional.

Notificaciones de Información

Los individuos deben recibir información acerca de cómo se tratarán sus datos personales , incluyendo los detalles relativos a:

- La identidad del responsable e información de contacto;
- Cualquier delegado de protección de datos;
- Las finalidades y bases legales para su tratamiento;
- Cualquier "interés legítimo" que sea la base del tratamiento;
- Cualquier transferencia internacional y garantías aplicables;
- El período de retención o los criterios para su determinación;
- El derecho a la portabilidad de datos y los derechos de oposición al tratamiento, de requerir la limitación y de retirar el consentimiento al tratamiento;
- El derecho a reclamar ante una autoridad de control; y
- Cualquier requisito legal o contractual para proporcionar datos, así como las consecuencias de no proporcionarlos.

La información debe de ser concisa, transparente e inequívoca, en una forma fácilmente accesible y con un lenguaje claro y sencillo, en particular cuando vaya dirigida a niños.

Cuando los datos personales sean obtenidos directamente, el responsable debe indicar qué información es obligatoria y las consecuencias de no proporcionarla. Cuando los datos personales sean obtenidos indirectamente, el responsable debe proporcionar la fuente de la información, incluyendo las fuentes accesibles al público.

Derecho de acceso

Los interesados tienen derecho a obtener copias de sus datos personales, junto con los detalles principales sobre cómo se tratan los datos. Los interesados han visto aumentados los derechos de acceso a sus datos:

- Los responsables ya no pueden cobrar una tarifa, pero pueden imponer un canon razonable por las copias adicionales.
- Los individuos deben dar detalles de las transferencias internacionales, los periodos de retención, los derechos de rectificación, supresión, limitación de tratamiento; y los derechos de oposición al tratamiento y de presentar una reclamación ante una autoridad de control.
- Los responsables deben revelar cualquier fuente de datos, la importancia y las consecuencias de cualquier tratamiento basado en decisiones automatizadas.

Derechos de los interesados

Los interesados tienen importantes derechos en relación a sus datos personales, incluyendo los siguientes:

- El derecho a exigir la rectificación de sus datos personales, sin dilaciones indebidas y el derecho a completar los datos personales que sean incompletos;
- El derecho a suprimir los datos personales ("derecho al olvido") cuando el tratamiento ya no sea necesario, el consentimiento sea revocado, los intereses legítimos ya no sean aplicables, el tratamiento sea ilegal, o la supresión se requiera por ley, y el responsable debe dar los pasos razonables para informar a otros responsables si ha hecho públicos dichos datos;
- El derecho a impedir tratamientos adicionales de datos personales ("limitación") cuando haya un conflicto en cuanto a su exactitud, cuando una oposición al tratamiento haya sido verificada, cuando el tratamiento sea ilegal y el interesado se oponga a la supresión, o cuando los datos ya no sean requeridos por el responsable, pero el interesado los requiera para la formulación, el ejercicio o la defensa de reclamaciones; y
- El derecho a exigir que los datos proporcionados por los interesados para su tratamiento con su consentimiento o bajo contrato puedan proporcionarse en una

forma de "*uso común y lectura por equipos y maquinas* " y transmitirse a otro responsable ("portabilidad de datos").

El responsable debe notificar a los destinatarios sobre cualquier rectificación, supresión y limitación salvo que le sea imposible o exija un esfuerzo desproporcionado. Además, si así lo solicita, el responsable debe comunicar a los interesados la identidad de los destinatarios.

Siguientes pasos

- ✓ Revisar las notificaciones de información y las políticas de privacidad.
- ✓ Revisión de los procedimientos de acceso de los interesados.
- ✓ Evaluar los métodos de cumplimiento de las solicitudes de portabilidad de datos y de limitación.
- ✓ Considerar las implicaciones del derecho al olvido para los sistemas de las tecnologías de la información (IT).
- ✓ Considerar formas de automatizar respuestas ante solicitudes individuales.

MECANISMOS DE GOBIERNO Y RENDICIÓN DE CUENTAS

ARTÍCULOS 24-25, 30, 32, 35, 37, 40 Y 42

Visión general: Las Nuevas Reglas

En contraste con la Directiva, el RGPD obliga a los responsables a implementar programas para garantizar el cumplimiento del RGPD y poderlo demostrar ante las autoridades de control e interesados.

Medidas técnicas y organizativas adecuadas

Los responsables deben implementar las medidas técnicas y organizativas adecuadas. Estas podrían incluir:

- La implementación de políticas de protección de datos;
- La adhesión a códigos de conducta aprobados; y
- La adhesión a mecanismos de certificación aprobados.

Protección de Datos por diseño y por defecto

Los responsables deben implementar las medidas técnicas y organizativas adecuadas, diseñadas para implementar los principios de protección de datos (tales como la seudonimización y la minimización de datos), ambas en el momento de determinar los medios de tratamiento así como durante el tratamiento en sí. Por defecto, solo deben ser tratados los datos personales necesarios para la finalidad específica.

Evaluación de impacto de protección de datos

Antes de que el tratamiento se efectúe, los responsables deben realizar una evaluación de impacto de las actividades que supongan riesgos importantes para los derechos de los interesados (por ejemplo, las decisiones basadas en el tratamiento automatizado o la elaboración de perfiles, el tratamiento a gran escala de datos sensibles y la observación sistemática a gran escala de una zona de acceso público).

Nombramiento del delegado de protección de datos

Los responsables y encargados deben designar un delegado de protección de datos ("DPO") si sus actividades principales requieren una observación habitual y sistemática de interesados a gran escala, o el tratamiento de datos sensibles a gran escala. Las autoridades u organismos públicos también han de designar un DPO. El nombramiento voluntario de un DPO es posible y, la legislación nacional puede exigir la designación de un DPO también en casos no específicamente descritos en el RGPD.

Documentación (registros de las actividades de tratamiento)

Los responsables deben mantener registros de las actividades de tratamiento que contengan cierta información requerida (incluyendo los fines de tratamiento, la descripción de las categorías de los interesados, los datos personales y los destinatarios, las medidas técnicas y organizativas implementadas, y cualquier transferencia de datos a terceros países).

Siguientes pasos

- ✓ Asignar la responsabilidad y establecer un presupuesto para el cumplimiento de la protección de datos y garantizar el apoyo de la alta dirección.
- ✓ Revisar el estado actual de cumplimiento. (Esto incluye la revisión de la protección de datos existente y de políticas de seguridad de las tecnologías de la información (IT) e identificar las actividades de tratamiento de datos relevantes).
- ✓ Realizar un análisis de las deficiencias con respecto a la rendición de cuentas en protección de datos.
- ✓ Actualización de los procedimientos existentes para garantizar el cumplimiento, y desarrollar nuevos procesos cuando sea necesario.
- ✓ Determinar si el nombramiento de un DPO es obligatorio, y en caso contrario, considerar la designación voluntaria del mismo.

OBLIGACIONES Y CONTRATOS DE ENCARGADO DE TRATAMIENTO

ARTÍCULOS 28 AL 33 Y 37

Visión general: Las Nuevas Reglas

El RGPD establece requisitos para los contratos entre los responsables y encargados de tratamiento de datos personales. Estos requisitos están más detallados que los contenidos en la Directiva.

Además, el RGPD establece nuevas obligaciones para los encargados.

Requisitos relativos a los contratos de tratamiento de datos para responsables y encargados

- Los responsables sólo deben recurrir a los encargados que ofrezcan garantías técnicas y organizativas suficientes de cumplimiento de los requisitos del RGPD.
- El contrato entre el responsable y el encargado debe constar por escrito.
- Los contratos de tratamiento deberán estipular lo siguiente:
  - El encargado solamente tratará los datos personales de acuerdo con las instrucciones del responsable;
  - El encargado debe asegurar que su personal está sujeto a una obligación de confidencialidad;
  - El encargado debe implementar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad de los datos personales apropiado al riesgo;
  - El encargado no puede subcontratar el tratamiento de datos personales sin la autorización previa y por escrito del responsable;
  - Cualquier contrato entre un encargado y un subencargado debe proporcionar las mismas obligaciones de protección de datos que las previstas en el contrato con el responsable;
  - El encargado debe asistir al responsable en garantizar el cumplimiento de las obligaciones de seguridad, la evaluación de impacto de protección de datos y la consulta previa a la Autoridad de Protección de Datos para el tratamiento de datos de alto riesgo;
  - El encargado debe suprimir o devolver los datos personales cuando el tratamiento se haya completado; y
  - El encargado debe proporcionar al responsable toda la información necesaria para demostrar el cumplimiento, así como permitir y contribuir a la realización de auditorías.

Obligaciones directas para los encargados

Excepto en casos limitados para las empresas u organizaciones que emplean a menos de 250 personas:

- el encargado debe mantener un registro por escrito de todas las categorías de tratamiento efectuadas por cuenta de un responsable; y
- el encargado pondrá dicho registro a disposición de la Autoridad de Protección de Datos que lo solicite.

Además, el encargado debe:

- Implementar las medidas técnicas y organizativas adecuadas para garantizar un nivel adecuado de seguridad;
- Adoptar medidas para asegurar que los miembros del personal con acceso a los datos personales los tratan únicamente de acuerdo con las instrucciones del responsable;
- Notificar al responsable sin dilación indebida después de tener conocimiento de una violación de la seguridad de los datos personales; y
- Designar un **DPO** en casos específicos incluso cuando: (i) el tratamiento requiera una observación regular y sistemática de interesados a gran escala, y; (ii) cuando los datos personales relativos a condenas e infracciones penales se traten.

Siguientes pasos

- ✓ Los responsables deben asegurar que todos los contratos con los encargados cumplen con los requisitos del RGPD.
- ✓ Los encargados deben determinar si los registros relativos al tratamiento para el responsable han de ser mantenidos.
- ✓ Los encargados deben implementar las medidas técnicas y organizativas adecuadas para garantizar un nivel adecuado de seguridad para los datos personales y deben implementar una política para notificar las violaciones de la seguridad de los datos personales.
- ✓ Los encargados deben determinar si es necesario la designación de un DPO.

SEGURIDAD DE LOS DATOS PERSONALES Y NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

ARTÍCULOS 32-34 Y 37

Visión general: Las Nuevas Reglas

Los encargados y responsables están ahora sujetos a un régimen de notificación de violación. Cuando sea posible, los responsables deben notificar las violaciones graves dentro de 72 horas.

Requisitos en materia de seguridad de datos

- Los responsables y encargados deben aplicar las medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel adecuado de protección de los datos personales.
- Cuando sea necesario, las medidas de seguridad deberán incluir la pseudonimización y el cifrado de datos personales, la capacidad de restaurar los datos personales de forma rápida y un proceso de verificación y evaluación regulares.
- Los responsables y encargados que realicen tratamientos y una observación de actividades a gran escala deberán designar un DPO.

Régimen de notificación de violación de la seguridad de los datos personales

Los encargados y responsables están ahora sujetos a un régimen de notificación de violación de la seguridad de los datos personales.

- Los responsables deben notificar las violaciones de la seguridad de los datos personales a la autoridad de control pertinente sin dilación indebida (cuando sea posible, dentro de las 72 horas posteriores a la detección de la violación), a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de los interesados.
- Los responsables deben notificar a los interesados afectados por la violación de sus datos personales cuando suponga un alto riesgo para los derechos y libertades de los interesados.
- Los encargados deben informar sobre las violaciones de la seguridad de los datos personales a los responsables sin dilación indebida y en todos los casos.

Siguientes pasos

- ✓ Implementar procedimientos para identificar los incidentes de seguridad, para dar respuesta a los mismos y realizar las necesarias notificaciones.
- ✓ Asignar la responsabilidad de la seguridad de los datos personales.
- ✓ Asegurar que los encargados están obligados a notificar las violaciones de la seguridad de los datos personales y a aplicar el nivel adecuado de seguridad.
- ✓ Comprobar la cobertura para los riesgos cibernéticos.
- ✓ Evaluar la seguridad y realizar regularmente pruebas.

CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

ARTÍCULOS 40-43

Visión general: Las Nuevas Reglas

El RGPD reconoce la aprobación de códigos de conducta y la acreditación de certificaciones, sellos y marcas, en particular a nivel de la UE, para ayudar a responsables y encargados para demostrar el cumplimiento de las normas de protección de datos. Los códigos de conducta, como se articulaban en la Directiva, jugaron un papel menos importante que el que se les atribuye en el RGPD. Bajo el RGPD, las certificaciones son reguladas por primera vez a nivel europeo.

Códigos de Conducta

- Bajo el RGPD, las asociaciones y otros organismos representativos pueden elaborar, modificar o ampliar un código de conducta con objeto de especificar como el RGPD se aplica a ciertos sectores de la industria.
- El código de conducta debe ser presentado ante la autoridad de control competente para su aprobación, registro y publicación.
- En caso de tratamiento internacional, el código de conducta debe presentarse al Comité Europeo de Protección de Datos ("el Comité") para que dé su opinión. La Comisión Europea ("Comisión") puede declarar que el código de conducta tiene validez general dentro de la UE. El Comité recopilará todos los códigos de conducta en un registro disponible al público.
- El cumplimiento con el código de conducta está sujeto a la supervisión de los organismos acreditados. En caso de infracción, la compañía en cuestión puede ser suspendida como entidad adherida al código y se notificará a las autoridades de control competentes.
- La adhesión a un código de conducta permite a los responsables y encargados de tratamiento ubicados fuera del Espacio Económico Europeo ("EEE") demostrar que han implementado las garantías adecuadas con el fin de permitir las transferencias de datos de los países del EEE a países fuera del EEE.

Mecanismos de certificación, sellos y marcas

- El establecimiento de mecanismos de certificación de protección de datos, sellos y marcas se promoverá con el fin de demostrar el cumplimiento del RGPD.
- La adhesión a los mecanismos de certificación, sellos y marcas permite a los encargados y responsables de tratamiento ubicados fuera del EEE demostrar que han implementado las garantías adecuadas para permitir las transferencias de datos de los países del EEE a países fuera del EEE.
- La autoridad de control competente o el Comité aprobarán los criterios para las certificaciones. El Comité podrá desarrollar criterios para una certificación única, por ejemplo, el Sello Europeo de Protección de Datos.
- Los organismos de certificación acreditados expedirán las certificaciones. Las acreditaciones de los organismos de certificación serán expedidas por un máximo de cinco años y están sujetas a renovación y revocación en caso de que las condiciones de acreditación dejen de cumplirse. Las certificaciones serán válidas por un máximo de tres años y pueden ser renovadas o revocadas cuando las condiciones para la emisión de la certificación hayan dejado de cumplirse.
- El Comité mantendrá un registro disponible al público de todos los mecanismos de certificación, sellos y marcas.

Siguientes pasos

- ✓ Identificar o establecer aquellas asociaciones u organismos representativos que pueden desarrollar códigos de conducta, en particular para las transferencias internacionales de datos.
- ✓ Supervisar la acreditación de los organismos de certificación y considerar la aplicación de las certificaciones.
- ✓ Entender los sistemas de certificación e indagar sobre las certificaciones, sellos y marcas a la hora de elegir a los proveedores de servicios.

TRANSFERENCIAS INTERNACIONALES DE DATOS

ARTÍCULOS 44-50

Visión general: Las Nuevas Reglas

Al igual que la Directiva, el RGPD requiere de una justificación adecuada para las transferencias de datos personales a países situados fuera del EEE. El RGPD ha ampliado las posibles justificaciones para las transferencias de datos mediante la inclusión de códigos de conducta y mecanismos de certificación aprobados.

- La Comisión puede adoptar decisiones de adecuación de terceros países, o territorios o sectores dentro de dichos países si se considera que ofrecen un nivel adecuado de protección para las transferencias internaci onales. Las transferencias a dichos países, territorios o sectores no requieren de autorizaciones específicas. La lista existente de terceros países considerados como adecuados por parte de la Comisión se mantiene en vigor e incluye el Escudo de privacidad UE-EEUU para las transferencias de datos de los países del EEE a los EEUU.
- En ausencia de una decisión de adecuación, los datos personales pueden ser transferidos a terceros países situados fuera del EEE sólo cuando se den las garantías adecuadas. Estas garantías incluyen las cláusulas contractuales tipo de protección de datos que pueden ser adoptadas o aprobadas por la Comisión, así como las Normas Corporativas Vinculantes ("NCV") cuyo contenido ha sido detallado en el RGPD. Otras transferencias sujetas a garantías específicas son aquellas permitidas en virtud de la existencia de un código de conducta válidamente aprobado, un mecanismo de certificación aprobado o un instrumento exigible entre las autoridades públicas esté en vigor.
- En ausencia de una decisión de adecuación o de garantías adecuadas, las transferencias internacionales son posibles bajo una de las siguientes condiciones: (i) el consentimiento explícito otorgado por el interesado después de que el interesado haya sido informado de los posibles riesgos de tales transferencias; (ii) la transferencia sea necesaria para un contrato o para la ejecución de medidas pre-contractuales entre el responsable y el interesado; (iii) la transferencia sea necesaria para un contrato concluido en interés del interesado entre el responsable y otra persona jurídica; (iv) la transferencia sea necesaria por razones importantes de interés público; (v) la transferencia sea necesaria para el reconocimiento, ejercicio o defensa de reclamaciones; (vi) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; y (vii) la transferencia se realice desde un registro público.
- El RGPD también se ocupa de situaciones de descubrimiento electrónico a terceros países (*e-discovery*) al indicar que las sentencias o decisiones de las autoridades administrativas de terceros países que requieran la transferencia de los datos personales pueden ser reconocidos o ejecutables sólo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua entre el país tercero requirente y la Unión Europea o un Estado miembro de la UE, sin perjuicio de los motivos mencionados anteriormente para la transferencia de conformidad con el RGPD.

Siguientes pasos

- ✓ Crear mapas de flujo de datos.
- ✓ Revisar las justificaciones legales para todas las transferencias internacionales existentes a países de fuera del EEE.
- ✓ Revisar el contenido de las NCV para garantizar el cumplimiento con los requerimientos del RGPD.
- ✓ Considerar nuevos motivos para las transferencias de datos, tales como códigos de conducta y certificaciones.
- ✓ Seguimiento de las novedades legislativas respecto a las decisiones de adecuación.

SUPERVISIÓN POR LAS AUTORIDADES DE PROTECCIÓN DE DATOS

ARTÍCULOS 51-76

Visión general: Las Nuevas Reglas

El RGPD establece normas detalladas y armonizadas aplicables a la organización y a los poderes de las autoridades de control. También prevé la cooperación y mecanismos de consistencia para abordar cuestiones relacionadas con los procedimientos internacionales.

Las Autoridades de Protección de Datos

Los Estados miembros mantendrán una o más Autoridades de Protección de Datos por país:

- La independencia de las Autoridades de Protección de Datos se verá reforzada por medio de las normas relativas al establecimiento de las Autoridades de Protección de Datos y las del nombramiento y cese de sus miembros, entre otras;
- Las funciones y competencias de las Autoridades de Protección de Datos se han ampliado, incluyendo la facultad de realizar auditorías y poder acceder a las instalaciones de los responsables y encargados.
- El RGPD establece un mecanismo de ventanilla única mediante el cual las Autoridades de Protección de Datos designan a una Autoridad de Protección de Datos principal (normalmente en base al lugar donde el encargado tenga su establecimiento principal) y cooperará para la adopción de decisiones relativas a transferencias internacionales de datos.

El Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos reemplazará al Grupo de Trabajo del Artículo 29:

- El Comité estará compuesto por el director de una Autoridad de Protección de Datos por cada Estado miembro y el Supervisor Europeo de Protección de Datos. Contará de una secretaría permanente proporcionada por el Supervisor Europeo de Protección de Datos y ubicada en Bruselas.
- El Comité emitirá dictámenes y directrices y garantizará la aplicación coherente del RGPD.
- El Comité dispone de poderes de decisión vinculantes en el caso de que existan diferencias entre las Autoridades de Protección de Datos en el procedimiento de ventanilla única (por ejemplo, acerca de cuál debería ser la Autoridad de Protección de Datos que deba ser la autoridad principal o en la determinación del contenido de la decisión final en la resolución de disputas).

Siguientes pasos

- ✓ Seguir los desarrollos legales nacionales que modifique la configuración institucional de las Autoridades de Protección de Datos.
- ✓ Entender los nuevos poderes extendidos de investigación de las Autoridades de Protección de Datos para las estructuras de cumplimiento interno.
- ✓ Determinar quien será la autoridad de control principal de la compañía.
- ✓ Prepararse para la posibilidad de intervenir ante el Comité y de recurrir sus decisiones.

RECURSOS, RESPONSABILIDADES Y SANCIONES

ARTÍCULOS 77-84

Visión general: Las Nuevas Reglas

El RGPD proporciona extensos recursos para los interesados y responsabilidades para los responsables y encargados, así como un aumento significativo de las sanciones, incluyendo multas similares a las del régimen de defensa de la competencia en la UE. A diferencia de la Directiva, el RGPD establece en detalle las condiciones para la imposición de multas, junto con sus cantidades máximas.

Reclamaciones

Los interesados tienen los siguientes derechos respecto de los responsables y encargados:

- Derecho a presentar reclamaciones (a través de las asociaciones representativas, entre otros medios) con las Autoridades de Protección de Datos en el Estado miembro en el que tenga el interesado su residencia, lugar de trabajo o el lugar de la infracción, incluyendo el recurso en caso de que la Autoridad de Protección de Datos no aborde la reclamación;
- Derecho a recurrir las decisiones vinculantes de las Autoridades de Protección de Datos ante los tribunales nacionales; y,
- Derecho a iniciar procedimientos judiciales ante los tribunales nacionales donde tengan su establecimiento el responsable o el encargado de tratamiento o donde el interesado tenga su residencia.

Indemnización y responsabilidad

Bajo el RGPD, el responsable y el encargado están obligados a compensar en su totalidad al interesado por el daño material e inmaterial que resulte como consecuencia de una infracción de las provisiones del RGPD. Esto también se aplica si hay más de un responsable o encargado, o ambos un responsable y un encargado, compartan la responsabilidad por los daños causados por el tratamiento ("responsabilidad solidaria").

Sanciones

Las Autoridades de Protección de Datos pueden imponer sanciones administrativas:

- Dependiendo del tipo de infracción, las sanciones podrían ser de hasta 20 millones de euros o, en el caso de que se trate de una empresa, hasta el 4% del volumen de negocios anual a nivel global, optándose por la cantidad que sea mayor.
- Las sanciones deben determinarse en base a los criterios enumerados en el RGPD y, están sujetas a revisión judicial y al correspondiente procedimiento.
- Los Estados miembros de la EU pueden imponer sanciones adicionales, incluso de carácter penal.

Siguientes pasos:

- ✓ Considerar nuevas responsabilidades y sanciones en la puesta a punto del cumplimiento.
- ✓ Evaluar la exposición a responsabilidades en virtud de acuerdos existentes con clientes/proveedores incluyendo una limitación de la responsabilidad a estos efectos.
- ✓ Determinar las jurisdicciones más probables para los procedimientos.
- ✓ Seguimiento de los desarrollos legislativos nacionales que creen sanciones adicionales.

GLOSARIO

Consentimiento del interesado	Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. **(Artículo 4, apartado 11, RGPD)**
Datos personales	Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador online o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. **(Artículo 4, apartado 1, RGPD)**
Destinatario	La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. **(Artículo 4, apartado 9, RGPD)**
Elaboración de perfiles	Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. **(Artículo 4, apartado 4, RGPD)**
Encargado de tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. **(Artículo 4, apartado 8, RGPD)**
Interesado	Una persona física identificada o identificable sobre la que los datos personales se están tratando. **(Artículo 4, apartado 1, RGPD)**
Normas Corporativas Vinculantes ("NCV")	Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la UE 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 **(Artículo 4, apartado 20, RGPD)**

GLOSARIO

Reglamento General de Protección de Datos ("RGPD")	Reglamento 2016/679/UE de 27 de Abril de 2016, que deroga la Directiva 95/46/CE, 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.
Responsable de tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales; cuando los fines y medios del tratamiento son establecidos por las leyes de la Unión Europea o de un Estado miembro de la UE, el responsable del tratamiento o los criterios específicos para su nombramiento, podrán ser establecidos por la legislación de la Unión Europea o del Estado miembro de la UE. **(Artículo 4, apartado 7, RGPD)**
Tercero	La persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable de tratamiento, del encargado de tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado. **(Artículo 4, apartado 10, RGPD)**
Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. **(Artículo 4, apartado 2, RGPD)**

INFORMACIÓN DE CONTACTO

Dr. Undine von Diemar
Múnich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathon Little
Londres
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Oberle-Robertson
Londres
+44.20.7039.5204
erobertson@jonesday.com

Olivier Haas
París
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Jörg Hladjk
Bruselas
+32.2.645.15.30
jhladjk@jonesday.com

Laurent De Muyter
Bruselas
+32.2.645.15.13
ldemuyter@jonesday.com

PUNTOS DE CONTACTO FUERA DE EUROPA

Daniel J. McLoon
Los Ángeles
+1.213.243.2580
djmcloon@jonesday.com

Aaron D. Charfoos
Chicago
+1.312.269.4242
acharfoos@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Guillermo E. Larrea
Ciudad de México
+52.55.3000.4064
glarrea@jonesday.com

Richard M. Martinez
Minneapolis
+1.612.217.8853
rmartinez@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
Nueva York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

Michiru Takahashi
Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com


JONES DAY
One Firm Worldwide℠