RGPD

Nota legal sobre el Reglamento General de Protección de Datos

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 27 de abril de 2016

NOTA LEGAL

ACERCA DE LAS OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES CON LA FUTURA NORMATIVA DEL RGPD Y CÓMO DEBE PROCEDER UNA ORGANIZACIÓN PARA OBTENER LA CONFORMIDAD.

DEFINICIONES

Responsable es la persona u organización que determina los fines y medios del tratamiento de los datos personales

Encargado es la persona u organización que procesa los datos personales en representación del responsable

Interesado es la persona cuyos datos personales se procesan

VERISEC

ÍNDICE

1. Sumario 3
2. Estado del RGPD 3
3. Ámbito del RGPD 4
4. Principios básicos 4
5. Consentimiento 5
6. Derechos del interesado 5
7. Responsabilidades del responsable y del encargado del tratamiento 6
8. Seguridad 6
9. Notificaciones de violación 7
10. Transferencia de datos personales a terceros países 7
11. Derecho a indemnización y responsabilidad 8
12. Resumen y análisis 8
13. Conclusiones 9

SUMARIO

Esta nota estudia la nueva normativa del RGPD promulgada el 27 de abril de 2016 y que entrará en vigor a partir del 25 de mayo de 2016.

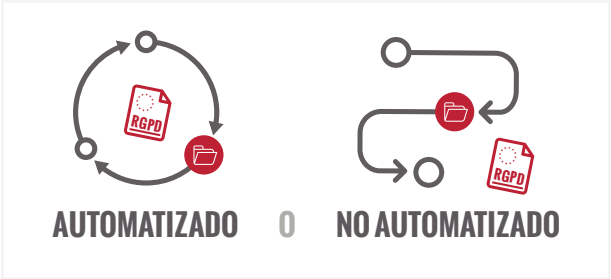
Todas las organizaciones que procesen datos relacionados con una persona identificada o identificable, denominada interesado, debe cumplir con el RGPD, y las consecuencias de no hacerlo pueden ser considerables. Las multas pueden alcanzar el 4 % del volumen de negocio global anual, o hasta 20 millones de Euros, lo que fuera superior.

El RGPD impone un número de obligaciones a responsables y encargados, y aunque el objetivo de estas normas es evidente, puede ser difícil entender cómo aplicarlas directamente en un escenario u organización. Examinaremos los principales requisitos y ofreceremos ayuda para comprender su implementación práctica. Esta nota incluye una lista de comprobación del RGPD que será de utilidad para que las organizaciones obtengan la conformidad.

> GDPR es un reglamento a nivel europeo, obligatorio en todos sus elementos y directamente aplicable en todos los Estados Miembros a partir del 25 de mayo de 2018

ÁMBITO DEL RGPD

El RGPD se centra en el tratamiento de datos a través de medios automatizados, pero también puede estar relacionado con los datos que forman parte de un sistema de archivo no automatizado.



En general, todo aquel que se ocupe del tratamiento de datos personales de ciudadanos europeos, ya sea que el responsable tenga o no su sede en la UE o que el tratamiento de los datos tenga lugar o no dentro de la UE, está sujeto a las normas del RGPD.

PRINCIPIOS BÁSICOS

El RGPD establece algunos principios básicos que se aplican a los datos personales.

En primer lugar, los datos se deben tratar de forma legal. En términos prácticos, esto significa que el interesado haya dado su **consentimiento** para el tratamiento de sus datos personales o que el tratamiento sea **necesario** para el cumplimiento de diversas obligaciones legales, ya sea del encargado o del interesado. La definición de consentimiento legal se examina en una sección posterior.

Los datos se deberán recopilar exclusivamente para fines específicos, explícitos y legítimos. Este principio se denomina limitación de la finalidad. Por lo tanto, se requiere la asignación de los activos de datos a una finalidad específica y legítima.

La minimización de datos significa que los datos tratados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Por lo tanto, más allá de vincular los activos a una finalidad, debemos establecer continuamente si los datos recopilados superan las pruebas de adecuación, relevancia y necesidad, y depurar los datos si no es así.

Los datos deben ser exactos y, si fuera necesario, actualizados, y lo datos inexactos se deben suprimir o rectificar. Para cualquier responsable del tratamiento de datos, esto es claramente una tarea compleja. Una forma de resolverla sería mediante el etiquetado de activos de datos o de categorías de activos susceptibles de cambiar a lo largo del tiempo, y mediante el establecimiento de un proceso de cambio para la actualización de estos activos de datos.

Los datos no se deberán conservar durante más tiempo del necesario. Esto significa que, una vez que la necesidad que fundamenta el tratamiento legal ha expirado, los datos se deben eliminar. Si la legalidad se basa en la necesidad, se deduce que los activos de datos se deben etiquetar con el motivo de esa necesidad, y que es necesario llevar a cabo un proceso de revisión similar al de exactitud para comprobar periódicamente que el criterio de legalidad se cumple.

SOLUCIÓN: Facilitar el filtrado mediante el etiquetado de datos

El responsable debe garantizar la seguridad de los datos personales a través de medidas técnicas y organizativas. **El reglamento menciona la integridad y confidencialidad de los datos; esto significa que los datos no se deben modificar y que se deben cifrar.** El RGPD establece expresamente que los activos de datos se deben cifrar, pero el cifrado por sí solo no es suficiente. **Es necesario implementar sólidos procesos, políticas y controles de gestión de claves para demostrar que los datos no se han perdido, dañado, alterado, destruido o procesado de manera ilegal.**

Aunque el cifrado solo se puede aplicar a través de medios técnicos, la gestión de claves puede, en teoría, llevarse a cabo mediante procesos, políticas y controles manuales. Sin embargo, en un entorno móvil y virtual complejo, un sistema automatizado que aplique las políticas, procedimientos y controles de gestión de claves resulta esencial.

CONSENTIMIENTO

El consentimiento debe darse mediante un acto afirmativo claro por parte del interesado. La normativa lo define como "una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen".[1]
Puede tratarse de una declaración oral o escrita, incluso se puede realizar mediante la activación de una casilla en un sitio web, **pero el consentimiento por defecto, por inactividad o mediante casillas pre-activadas, no constituye un consentimiento.**

DERECHOS DEL INTERESADO

The data subject has a number of rights that are defined by GDPR. These rights pose some practical problems for the controller and processor in terms of quickly identifying and retrieving the relevant data assets in order to take a required action on them. Some of the key ones to bear in mind is mentioned below.

El derecho de acceso otorga al interesado el derecho a obtener confirmación de si se están tratando o no datos personales que le conciernen, la finalidad del tratamiento, la categoría de los datos, el destinatario al que se comunicarán los datos, la existencia de decisiones automatizadas que se basen en los datos y el periodo durante el cual se almacenarán los datos. Por lo tanto, los responsables deben agregar etiquetas adicionales a los datos personales de manera que sea posible la recuperación y presentación rápidas de esta información adicional.

El interesado tiene derecho a la supresión, esto es, el derecho a pedir la eliminación de los datos cuyo consentimiento de tratamiento haya retirado o cuyo tratamiento ya no sea necesario. Como se mencionó anteriormente, esto requiere que el encargado pueda recuperar rápidamente un inventario de activos de datos y pueda establecer cuáles se deben suprimir.

El derecho a la portabilidad de los datos significa que el interesado tendrá derecho a recibir, cuando así lo desee, los datos personales que le incumban, en un formato de lectura mecánica. Este derecho también se encamina a posibilitar que el interesado pueda transmitir todos sus datos personales de forma sencilla a un nuevo responsable y encargado del tratamiento de datos.

[1] (32) del preámbulo del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 27 de abril de 2016

RESPONSABILIDADES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO

El RGPD detalla las responsabilidades del responsable y del encargado. A continuación, enumeramos las principales.

El encargado del tratamiento no recurrirá a otro encargado sin autorización del responsable. Hay requisitos detallados en lo que se refiere a la relación contractual entre un responsable y un encargado del tratamiento.
Los responsables tienen la obligación de mantener registros de las actividades de tratamiento. Se adjunta a este documento una plantilla de los registros exigidos.

SEGURIDAD

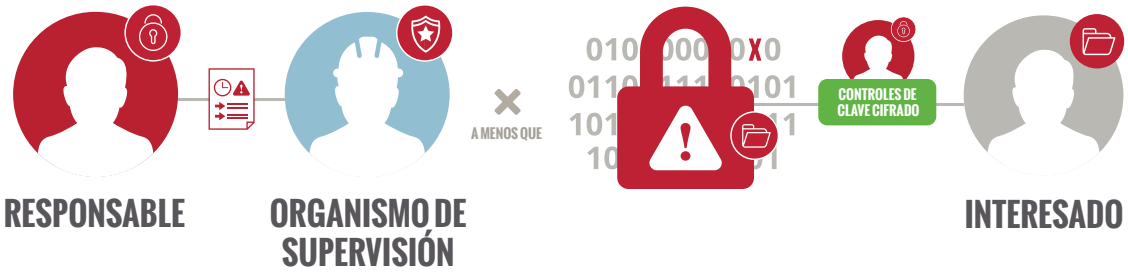
Los responsables tienen la obligación de garantizar la seguridad de los datos tratados, en concreto, a través del cifrado.
El responsable deberá aplicar al tratamiento de los datos los principios de protección de datos desde el diseño y por defecto, las obligaciones y los derechos de los interesados tal y como se describen en esta nota. Esto significa que, por ejemplo, el sistema se debe diseñar de acuerdo al principio de minimización de datos; en otras palabras, solo se deben almacenar los datos que sean adecuados, pertinentes y limitados a lo necesario. El cumplimiento de estas obligaciones será un atenuante de las responsabilidades en caso de violación, y no hacerlo es, en sí mismo, una violación del reglamento y podría implicar responsabilidad.

Una cualificación importante y explícita es que el responsable y el encargado deberán llevar a cabo las acciones necesarias para asegurarse de que las personas que actúen bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo puedan tratar dichos datos siguiendo instrucciones del responsable. Este último requisito solo se puede conseguir de manera razonable a través de la adopción de sólidas prácticas y controles de gestión de claves, ya sean organizativas o automatizadas.

NOTIFICACIONES DE VIOLACIÓN

En el caso de una violación de seguridad, el responsable tiene la obligación de informar de tal violación a los organismos de supervisión, a menos que sea improbable que la violación de los datos personales ponga en riesgo los derechos y libertades de las personas naturales. En la práctica, esto se traduce en que, si la violación se produce cuando los datos están cifrados, no es necesaria la notificación.3

El principio anterior también se aplica a la obligación de notificar al interesado. En ambos casos, la capacidad para determinar la baja probabilidad de que la violación genere un riesgo también depende de los controles de las claves de cifrado disponibles para el responsable, ya que el valor de un sistema de cifrado es tan fuerte como la gestión de sus claves.



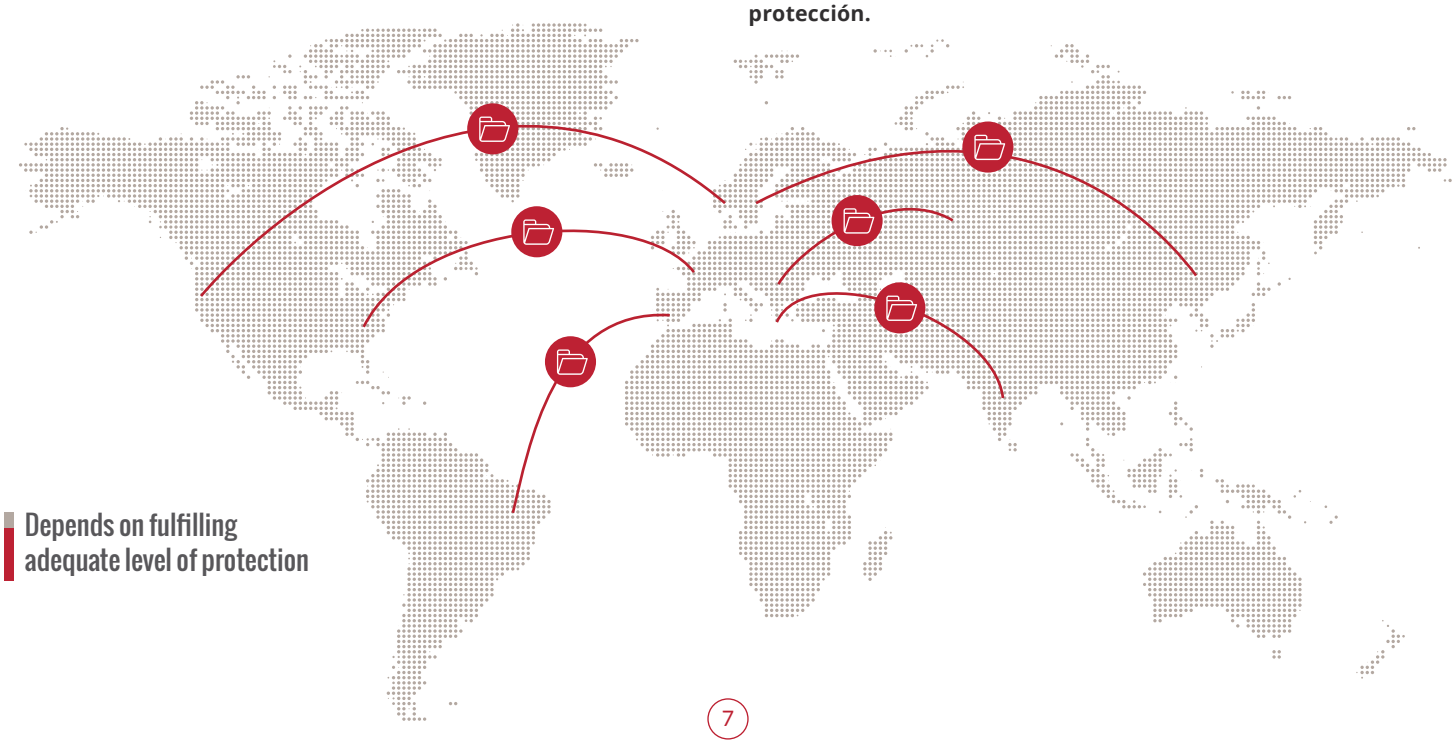
[3] Aunque esa excepción no se formula explícitamente, Verisec ha buscado una opinión legal externa en esta tema, que confirma la afirmación de que el responsable queda eximido de la obligación de notificación si los datos perdidos o sustraídos están cifrados.

TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES

El requisito básico para las transferencias a terceros países es que la Comisión haya considerado que el país en cuestión garantiza un nivel adecuado de protección.

La Comisión deberá publicar en el Diario Oficial de la Unión Europea y en su sitio web la lista de los terceros países pertinentes.
Cualquier sentencia de un tribunal y cualquier decisión de un organismo administrativo de un tercer país que requiera que un responsable o encargado transfiera o divulgue datos personales, solo será reconocible o exigible de alguna manera si se basa en un acuerdo internacional entre ese país y la Unión Europea.

Depende del cumplimiento de un adecuado nivel de protección.



DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD

Los interesados que hayan sufrido daños y perjuicios como consecuencia de una infracción del RGPD tienen el derecho de recibir una compensación por los daños sufridos, y la responsabilidad por el daño causado recaerá sobre el responsable pertinente.

El nivel de responsabilidad dependerá de la naturaleza y gravedad de la infracción y de su intencionalidad o negligencia, así como de otras consideraciones. Sin embargo, el punto determinante para la atenuación de la responsabilidad es la capacidad para demostrar que esa acción se ha llevado a cabo para cumplir con los principios básicos y con las responsabilidades generales del responsable.

El responsabilidad más alta, el 4 % del volumen de negocio total anual global o 20 000 000 EUR, el que sea más alto, se reserva para las infracciones de los principios básicos, de los derechos de los interesados y de las normas relacionadas con la transferencia de los datos personales a terceros países.

Se aplica una responsabilidad más baja, con una cuantía del 2 % del volumen de negocio total anual global, a infracciones de menor gravedad, incluido el diseño deficiente del sistema de tratamiento.

RESUMEN Y ANÁLISIS

El RGPD requiere que los responsables y encargados lleven a cabo una inventario más granular de sus activos de datos del que suele estar disponible actualmente, a fin de cribar los datos a lo largo del tiempo y mantenerlos actualizados. Este inventario es asimismo esencial para cumplir rápidamente con los derechos de los interesados que se establecen en el reglamento.

La tecnología de cifrado es un requisito explícito, pero también lo es la capacidad para determinar que únicamente las personas autorizadas tengan acceso a los datos cifrados. Esta es una tarea difícil y compleja de lograr a través de políticas y procedimientos manuales; por lo tanto, se requieren sistemas automatizados que apliquen las políticas digitalmente.

CONCLUSIONES

La clave para la conformidad es, en primer lugar, esforzarse en poner en marcha un inventario exhaustivo de las categorías de activos de datos y un número de etiquetas de clasificación relacionadas con el tiempo, la legalidad, la finalidad, etc., sobre las que se pueda aplicar búsquedas y auditorías con facilidad. Se incluye a continuación una plantilla de etiquetas relevantes para datos. **Es necesario que estas etiquetas se puedan buscar y auditar fácilmente, y que los datos subyacentes sean suprimibles, modificables y transferibles.**

Otro punto esencial en el RGPD es el cifrado y la gestión de claves. Un sistema automatizado de cifrado y gestión de claves que aplique los controles, procedimientos y políticas de la gestión de claves es, probablemente, la única forma de cumplir con la normativa en un entorno cada vez más complejo, con volúmenes de datos en crecimiento y dispositivos que los consumen y almacenan.

Verisec es un proveedor tecnológico en las áreas de cifrado, gestión de claves e identidad digital móvil; su objetivo es garantizar la protección de los datos y que únicamente las personas autorizadas tengan las claves para obtener acceso a los activos de datos.

Acerca de Verisec

Verisec es una compañía de vanguardia en seguridad digital que crea soluciones para mejorar la seguridad y el acceso a los sistemas. Ofrecemos una amplia gama de productos y servicios en nuestras dos áreas de negocio: identidad digital y seguridad de la información. Verisec lleva a cabo operaciones y distribución a nivel global con oficinas en Estocolmo, Londres, Belgrado, Madrid, Ciudad de México, Dubái y Frankfurt. Verisec cotiza en el mercado Nasdaq First North de Estocolmo desde 2014.

www.verisec.com