



ACT Enterprise de Vanderbilt

Reglamento General de Protección de Datos de la UE: guía de cumplimiento

Contenido

Resumen.....	2
Descripción general.....	2
¿Qué son los datos personales?.....	2
¿En qué consiste el tratamiento de datos?	3
¿Actúo como responsable o encargado del tratamiento?	3
¿Qué es el consentimiento del interesado y es necesario tenerlo en cuenta?	3
¿Qué es un contrato de tratamiento de datos y es necesario tenerlo en cuenta?.....	4
Conozca su papel y su responsabilidad	4
ACT Enterprise y RGPD	5



Resumen

Con las soluciones y productos de Vanderbilt, los clientes pueden gestionar y tratar los datos personales de modo que respetan los requisitos del RGPD. El objetivo de esta guía es ayudar a nuestros clientes a evaluar si están o no preparados para cumplir con sus responsabilidades y obligaciones con respecto a los nuevos reglamentos.

Descripción general

La protección de datos es un derecho fundamental por el que todo el mundo tiene el derecho a que sus datos personales estén protegidos. El Reglamento general de Protección de Datos (RGPD) se aplica a partir del 25 de mayo de 2018 y está elaborado para que las personas tengan más control sobre sus datos personales. Existe un conjunto de normas para toda la UE y pueden complementarse en algunas áreas con la legislación nacional.

El RGPD impone obligaciones a las empresas y organizaciones que recogen, utilizan y tratan datos personales. El requisito central del RGPD para las organizaciones y empresas es ser totalmente transparentes sobre la forma en que utilizan y protegen los datos personales y poder asumir la responsabilidad de sus actividades de tratamiento de datos. Estos datos se tratarán de forma leal para fines específicos y sobre la base del consentimiento del interesado o de cualquier otra base legítima establecida por la ley.

Aunque Vanderbilt ofrece a los clientes una funcionalidad de productos flexible e intuitiva para facilitar el cumplimiento de los nuevos reglamentos, la organización de Vanderbilt ni recoge ni controla ni utiliza ni trata los datos personales que existen en los productos de las instalaciones propias de Vanderbilt. Por tanto, es responsabilidad del responsable y del encargado del tratamiento de asegurar que las obligaciones indicadas en el RGPD se cumplan.

En caso de cualquier duda o de no conocer con certeza la identidad del responsable del tratamiento o del encargado del tratamiento, debe consultar con el asesor jurídico.

¿Qué son los datos personales?

El término «datos personales» significa cualquier información relativa a una persona viva que está identificada o es identificable.

Una persona es identificable si puede ser identificada directa o indirectamente mediante un «identificador». El RGPD da ejemplos de identificadores, como nombres, números de identificación y datos de localización. Una persona también puede ser identificada mediante elementos propios de la identidad física, genética o cultural.

Los datos personales que se han sometido a despersonalización, cifrado o seudonimización y que pueden utilizarse para identificar de nuevo a una persona siguen siendo datos personales y entran en el ámbito del RGPD. Si los datos personales se han convertido en anónimos de modo que la persona ya no es identificable, entonces dejan de considerarse datos personales. Para que los datos sean completamente anónimos, el proceso debe ser irreversible.

La ley protege los datos personales independientemente de la tecnología o el método utilizado para el tratamiento de los datos: se aplica tanto al tratamiento automatizado como manual. Tampoco importa el modo en que se conservan los datos personales (sistema informático, videovigilancia o



papel); en todos los casos, los datos personales están sujetos a los requisitos de protección descritos en el RGPD.

¿En qué consiste el tratamiento de datos?

El tratamiento abarca diversas operaciones realizadas en los datos personales por medios manuales o automatizados. Incluye 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 de los datos personales.

El Reglamento General de Protección de Datos (RGPD) se aplica al tratamiento de todos o parte de los datos personales por medios automatizados y manuales, si forma parte de un fichero estructurado.

¿Actúo como responsable o encargado del tratamiento?

Un responsable del tratamiento es la persona o persona jurídica que controla y es responsable de guardar y utilizar la información personal en un ordenador o en archivos manuales estructurados. Ser responsable del tratamiento implica responsabilidades legales, de modo que debe tener claro si estas responsabilidades se aplican a usted o su organización.

Si usted o su organización controla y es responsable de los datos personales que conserva, es decir, decide qué información personal se conservará y qué uso se le dará, entonces usted o su organización es un responsable del tratamiento.

Ejemplos de casos en los que el responsable del tratamiento es una persona son médicos, farmacéuticos, políticos y comerciantes individuales, cuando esas personas conservan información personal de sus pacientes, clientes, electores, etc.

Si usted o su organización conserva los datos personales, pero otra persona y organización decide y es responsable de lo que ocurre con esos datos, entonces esa persona u organización es el responsable del tratamiento y usted o su organización es el «encargado del tratamiento».

Ejemplos de encargados del tratamiento son empresas encargadas del pago de nóminas, gestores financieros y empresas de investigación de mercado, los cuales pueden conservar o tratar la información personal en nombre de otro.

¿Qué es el consentimiento del interesado y es necesario tenerlo en cuenta?

Para tratar legalmente los datos personales, las organizaciones y empresas deben identificar y documentar la base legal para ello desde el principio. Algunas de las formas legales para tratar los datos son:

- **Consentimiento del interesado:** el consentimiento es adecuado si las personas pueden elegir realmente y tienen el control sobre el modo en que se utilizan sus datos.
- **Intereses vitales:** el tratamiento es necesario para proteger los intereses vitales de la persona, por ejemplo, en caso de ser necesario proteger su vida.
- **Cumplimiento con una obligación legal:** los datos pueden tratarse si, por ejemplo, la ley europea lo exige por un motivo particular.



- **Un contrato con el interesado:** el tratamiento es necesario para ejecutar un contrato con una persona, por ejemplo, suministrar bienes o prestar servicios que han sido solicitados.

En caso de dudar de si cuenta con el consentimiento suficiente para tratar los datos personales, debería consultar con su asesor jurídico.

¿Qué es un contrato de tratamiento de datos y es necesario tenerlo en cuenta?

Si almacena o trata (introduce, edita, conserva) datos personales (encargado del tratamiento) en nombre de su cliente (responsable del tratamiento), necesitará un contrato para el tratamiento de los datos. Le recomendamos que se asesore legalmente para asegurarse de que el contrato contemple las cuestiones de seguridad y otras garantías adicionales de protección de los datos. Como parte que somos, recomendamos a los clientes que cuenten con una lista de comprobación relativa al tratamiento de los datos y al traspaso del sistema de seguridad.

Conozca su papel y su responsabilidad

Está claro que la ley está cambiando al RGPD y que debe ser integrado en la planificación de los sistemas de seguridad. Se deben identificar y abordar las áreas que pueden provocar problemas de cumplimiento según el RGPD. En el RGPD, los interesados tienen el derecho de recibir información clara sobre la utilización de sus datos.

El primer paso práctico es identificar su papel y responsabilidad con respecto al RGPD. ¿Es usted responsable del tratamiento, encargado del tratamiento o ambas cosas? En caso de cualquier duda o de no conocer con certeza la identidad del responsable del tratamiento o del encargado del tratamiento, debe consultar con el asesor jurídico.

El segundo paso es asumir la responsabilidad. Tenga en cuenta todos los datos personales que manipula cuando trabaja con el sistema de seguridad y analícelos según las siguientes categorías:

- ¿Qué datos personales se conservan?
- ¿Cuál es la base legal en la que se basa el tratamiento de los datos personales?
- ¿Dónde se conservan los datos?
- ¿Cómo se protegen los datos?
- ¿Durante cuánto tiempo se conservan los datos?
- ¿Cuál es la política para tratar las solicitudes de acceso a los datos personales?
- ¿Cuál es el procedimiento en caso de que alguien pida que se eliminen sus datos del sistema?
- ¿Quién tiene acceso a los datos?
- ¿Se transfieren los datos fuera del EEE?



ACT Enterprise y RGPD

La siguiente información describe cómo puede usarse el sistema ACT Enterprise de Vanderbilt para facilitar el cumplimiento del RGPD.

¿Qué datos personales se conservan?

No es necesario conservar ningún dato personal para que el sistema ACT Enterprise funcione correctamente.

Los campos de imagen, nombre, dirección electrónica y número de teléfono están predefinidos, pero se pueden usar campos definibles por el usuario para introducir distintos datos personales.

¿Cuál es la base legal en la que se basa el tratamiento de los datos personales?

La introducción de los datos y el mantenimiento de los datos están controlados por el responsable del tratamiento y el encargado del tratamiento del centro. Como tales, es responsabilidad del responsable del tratamiento o del encargado del tratamiento garantizar la base legal para el tratamiento de los datos personales.

No existe ningún procedimiento explícito integrado en el software ACT Enterprise para obtener el consentimiento del usuario o grabarlo.

¿Dónde se conservan los datos?

Los datos se conservan en la base de datos de ACT Enterprise ubicada en el servidor y en las copias de seguridad. Puede haber datos personales conservados en los controladores del sistema (nombres), pero el propietario del sistema puede desactivar esta opción.

¿Cómo se protegen los datos?

Para acceder al contenido de la base de datos de ACT Enterprise, se utiliza el software del cliente (ACT Manage, Monitor o Install). El inicio de sesión en el software está protegido con contraseña.

No ciframos los datos personales. El usuario final puede elegir forzar el cifrado a nivel de la base de datos (SQL Server o SQL Compact).

El personal de Vanderbilt no tiene acceso al sistema del cliente, a menos que sea autorizado a través del inicio de sesión remoto.

¿Durante cuánto tiempo se conservan los datos?

En ACT Enterprise, los datos del titular de la tarjeta se conservan mientras la persona necesite la tarjeta. Se puede definir la fecha de caducidad de la tarjeta, pero es el usuario del sistema el que debe eliminar los datos del titular de la tarjeta cuando caduque. Vanderbilt ofrece un informe de caducidad de tarjetas para facilitar este proceso.

Disponemos de una función para purgar los eventos de registro anteriores a un periodo de meses establecido y que el usuario puede personalizar. De forma predeterminada, los eventos se guardan para siempre.

De forma predeterminada, al eliminar a un titular de tarjeta, el sistema no elimina los eventos de registros relacionados aunque puede modificarse esta opción para eliminar los eventos de registro al eliminar al usuario.



¿Cuál es la política para tratar las solicitudes de acceso a los datos personales?

Si existe una solicitud, es responsabilidad del responsable del tratamiento o del encargado del tratamiento de definir la política y aportar los datos de forma rápida de acuerdo con el RGPD.

En ACT Enterprise existen varios informes para detallar la información existente sobre una persona, como los eventos de registro recientes, y una manera de exportar esos informes a archivos PDF estándar o archivos CSV.

¿Cuál es el procedimiento en caso de que alguien pida que se eliminen sus datos del sistema?

Si existe una solicitud, es responsabilidad del responsable del tratamiento o del encargado del tratamiento de definir la política y eliminar los datos de forma rápida de acuerdo con el RGPD.

El usuario final puede eliminar manualmente del sistema ACT Enterprise los datos del titular de la tarjeta. De forma predeterminada, el sistema no elimina los datos de eventos de registro asociados. Pero se pueden modificar los ajustes de modo que los eventos de registro de los usuarios eliminados también se eliminen.

¿Quién tiene acceso a los datos?

Es responsabilidad del responsable del tratamiento o del encargado del tratamiento comunicar quién tiene acceso a los datos personales en el sistema ACT Enterprise instalado en el centro. El responsable del tratamiento o del encargado del tratamiento es responsable de crear y aplicar estos procedimientos.

Enterprise tiene un sistema de usuarios de la base de datos para otorgar a personas determinadas derechos sobre el software cliente. Se controlan todos los accesos al sistema, desde inicios de sesión, cambios de los datos de usuario y acciones.

¿Se transfieren los datos fuera del EEE?

En el modo de funcionamiento normal, los datos del usuario de ACT Enterprise no se comparten fuera del sistema. Es responsabilidad del responsable del tratamiento o del encargado del tratamiento comunicar si el sistema está configurado de modo que transfiera datos fuera del EEE.