safetica

Cómo usar Safetica para cumplir con la GDPR

6. 6. 2023

Introducción

¿Qué es la GDPR?

GDPR es el reglamento de la Unión Europea 2016/679 relativo a la protección de las personas físicas en relación con el tratamiento de datos personales y a la libre circulación de estos datos. La GDPR entra en vigor en toda la UE el 25 de mayo de 2018. Sustituirá tanto a la actual Directiva 95/46/ES como a las actuales leyes de protección de datos personales en toda la Unión en todos los países de la UE.

Los requisitos más importantes de la GDPR

- Establecer una base legal para el tratamiento de datos personales.
- Especificar la finalidad del tratamiento de la información personal.
- Establecer el tiempo de retención de datos y los derechos de acceso adecuados para el manejo de datos personales.
- Mantener registros del manejo de datos.
- Garantizar la seguridad de los datos personales.
- Generar documentación completa de todos los procedimientos organizativos que puedan ser utilizados como guía de usuario y que servirán como punto de partida durante un incidente de seguridad.
- Proporcione a los empleados formación sobre todos los procesos de datos de la organización y sobre cómo trabajar de forma segura con datos confidenciales.
- Asegúrese de que se atiendan los derechos de todos los interesados.
- Bajo ciertas condiciones, asigne un Delegado de Protección de Datos (DPO).
- Es posible que se necesite una evaluación de impacto (EIPD) (capítulo 4, sección 3) en el caso de que una empresa lleve a cabo un amplio procesamiento automatizado de datos o perfiles de comportamiento.
- Haber celebrado contratos, revisados de acuerdo con la GDPR, con personas con las que se comparte información personal.

- Notificar por escrito a los interesados (empleados) sobre el tratamiento de sus datos personales de acuerdo con el Derecho a la información.

Protección de datos y pasos necesarios para el cumplimiento de la GDPR

¿De qué se encarga Safetica?

Safetica se basa en una tecnología que recopila los registros registrados en las estaciones de punto final. Incluye información sobre el uso de la computadora, sobre aplicaciones, sitios web, dispositivos conectados, mensajes de correo electrónico, impresión, tráfico de red, operaciones de archivos, etc. Debido a que estos registros se guardan en una base de datos, es necesario tomar medidas para garantizar que Safetica y el entorno en el que se utiliza cumplan con la GDPR.

Pasos clave para el cumplimiento de la GDPR

Seguridad del medio ambiente

Se recomienda encarecidamente utilizar un servidor dedicado para Safetica Management Service (SMS) con el fin de aumentar la seguridad y reducir los riesgos de posibles amenazas.

Recomendamos que el acceso de administrador a las bases de datos de Safetica se limite al número mínimo de administradores necesarios, que mantengan el buen funcionamiento y la disponibilidad de los servicios.

Después de instalar Safetica, es necesario definir las cuentas de usuario individuales y los derechos de acuerdo con los roles de la empresa y los principios recomendados:

- Principio de privilegios mínimos: todos los usuarios deben iniciar sesión con una cuenta de usuario que tenga los permisos mínimos absolutos necesarios para completar la tarea actual y nada más.

- Distribución de roles: cada usuario debe desempeñar un rol específico en el sistema. El administrador debe tener privilegios para configurar el producto, no para ver registros. Gestiona exactamente lo contrario.
- No recomendamos utilizar la cuenta del sistema de Safetica para ningún otro propósito que no sea la asignación de roles.

Safetica utiliza un producto de terceros (Microsoft SQL Server) para almacenar sus datos. Su funcionalidad y retención de datos deben gestionarse adecuadamente y la seguridad debe configurarse de manera que se minimice cualquier riesgo de violación de los datos personales almacenados en ella. Puede encontrar más detalles en el documento "Recomendaciones posteriores a la implementación".

Recomendaciones generales para garantizar la seguridad de los datos:

- Acceso físico seguro a todos los archivos y servidores de la base de datos
- Asegurar la CIA (Confidencialidad, Integridad, Disponibilidad) de los datos tratados
- Opcional: MSSQL Enterprise Edition
- Opcional: Uso del protocolo IEEE 802.1X

Obligaciones y responsabilidades legales en virtud de la GDPR

Si una empresa cumple con las siguientes condiciones, la empresa debe nombrar un DPO (Delegado de Protección de Datos). Un DPD es responsable de supervisar tanto la estrategia de protección de datos como su implementación para garantizar el cumplimiento de los requisitos dla GDPR. El nombramiento de un DPD solo es obligatorio en tres situaciones:

- La organización es una autoridad pública
- Las actividades principales de la organización consisten en operaciones de procesamiento de datos que requieren un seguimiento regular y sistemático de los interesados a gran escala
- Existe un tratamiento a gran escala de categorías especiales de datos (es decir, datos sensibles como la salud, la religión, la raza, la orientación sexual, etc.) y datos personales relacionados con condenas y delitos penales.

La solución Safetica puede, en casos excepcionales, requerir el nombramiento de un DPO, dependiendo del tipo de empresa y del ámbito de uso. Para una evaluación específica, recomendamos consultar a un abogado corporativo.

En el caso de un tratamiento automatizado de datos o de elaboración de perfiles de gran envergadura, se recomienda realizar una evaluación de impacto (EIPD) (capítulo 4, sección 3) para determinar la gravedad del impacto. Recomendamos que la EIPD se implemente en consulta con la representación legal. En determinados casos en los que no sea posible reducir suficientemente los riesgos, el responsable del tratamiento está obligado a informar a la autoridad de control. Safetica puede, en función del ámbito de uso (en virtud del artículo 35, apartado 3, letra a)), exigir la aplicación de la EIPD. Para una evaluación específica, recomendamos consultar con un asesor legal.

Documentación requerida por la GDPR

- Si los datos de Safetica son procesados por una entidad externa, como un socio de Safetica, debe firmar un contrato de procesamiento de datos, como se describe en el artículo 28 dla GDPR. El contrato debe abordar todas las estipulaciones necesarias que se describen en él.
- Al igual que con cualquier software de seguridad utilizado en una empresa, la información sobre Safetica debe incluirse en la política de seguridad de la empresa.
- La empresa debe notificar por escrito a los empleados antes de utilizar Safetica. Este aviso debe contener la información descrita en el artículo 13 dla GDPR.
- En su caso, también es obligatorio mantener registros del tratamiento de datos personales en virtud del artículo 30 dla GDPR.

El acceso de los usuarios individuales y las modificaciones de configuración se registran automáticamente en Safetica en el modo de visualización Mantenimiento > Cuentas de usuario.

Los derechos de los interesados

un. El derecho a la información y el derecho de acceso (capítulo 3, sección 2, artículos 13 a 15)

- Si un interesado reclama el derecho a la información, puede crear una tabla estructurada para él. Un ejemplo de una tabla de este tipo se puede encontrar en el capítulo "Apéndice". La solicitud de información también se puede gestionar mediante la presentación de una notificación por escrito (como se ha comentado anteriormente en la sección 6 c) de "Documentación requerida").

- Además de proporcionar una descripción general de los datos procesados, también debe incluir la información de contacto de la persona responsable del procesamiento de datos.

	Título	Apellido	Nombre	Correo electrónico	Teléfono
Administrador					
Administrador Adjunto*					
DPO*					

**Cuando corresponda*

- Durante un tiempo dentro del período de retención, puede ejercer el derecho de acceso proporcionando información específica sobre el procesamiento de datos al interesado en forma de un informe de Safetica, o mostrando los datos en la consola de Safetica.

b. Derecho a la portabilidad de los datos (Capítulo 3, Sección 2, Artículo 20)Este derecho no se aplica a Safetica debido a la base jurídica aplicable (interés legítimo en la protección de la propiedad intelectual de una empresa, que entra en el ámbito de aplicación del artículo 6, apartado 1, letra f), sobre la base del preámbulo (49)).

c. El derecho a restringir el procesamiento (Capítulo 3, Sección 3, Artículo 18)Un administrador puede eliminar los permisos para ver los datos procesados de los interesados de Safetica para todas las cuentas de usuario que se vean afectadas por la solicitud.

d. El derecho de rectificación (Capítulo 3, Sección 3, Artículo 16)Los datos están vinculados al interesado por su nombre de dominio y su nombre de ordenador. Un administrador puede cambiar el nombre del interesado en el árbol de usuarios.

e. El derecho de supresión (Capítulo 3, Sección 3, Artículo 17)

Para cumplir con este derecho, debe eliminar usuarios del árbol de usuarios en la consola de Safetica. Los datos archivados deben eliminarse cuando expire el período de retención. Se recomienda un tiempo de retención de seis meses. Se pueden establecer otros plazos de prescripción y revocación, con un plazo de hasta 15 años o más en algunos países.

f. Derecho de oposición (Capítulo 3, Sección 4, Artículo 21)

Los socios de Safetica pueden proporcionar servicios (como la realización de un análisis de seguridad) a los clientes de Safetica. Se trata de una relación contractual que permite al tercero (el socio) acceder a los datos de Safetica con el fin de prestar su servicio.

Esta relación debe describirse en una política de seguridad o en un aviso por escrito.

En el caso de que un interesado reclame el derecho a oponerse a los datos relacionados, recomendamos señalar la política de seguridad de la empresa y discutir el objetivo principal del producto, que es proteger los activos de la empresa y respaldar los requisitos dla GDPR.

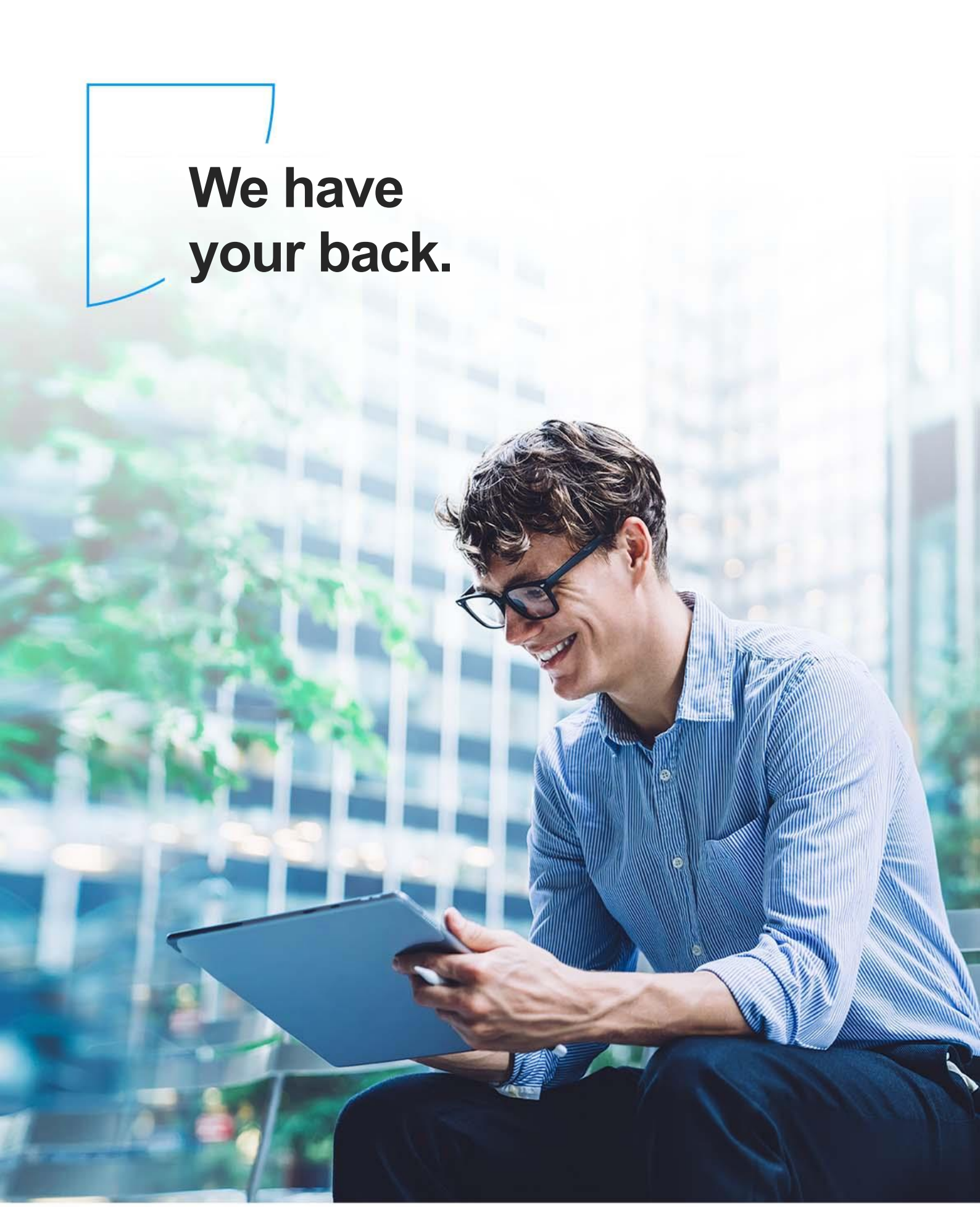
Anexo: tabla de muestra de tratamiento de datos personales

Objeto del tratamiento de datos	Empleados de la empresa / Modificar según los datos de su empresa
Descripción	Datos descriptivos, registros sobre los datos y el software a los que se accede en los hosts de la empresa, el uso de Internet y de la red en general, el uso de la impresora y otros dispositivos de E/S, las operaciones realizadas en los hosts de la empresa, los registros de errores y depuración de los hosts y el software de la empresa
Finalidad del tratamiento de los datos	Interés legítimo de proteger los activos de la empresa, incluidos, entre otros, la propiedad intelectual y la mejora de la seguridad de la empresa.
Base jurídica (licencias) de conformidad con los artículos 6 y 9	6, apartado 1, letra f) Interés legítimo
Propietario (persona responsable internamente)	Especifique de acuerdo a su empresa
Periodo de conservación	Durante la duración del contrato de trabajo + 6 meses / especificar según su empresa
Método de retención de datos	Sistema Safetica, sistema de base de datos, copias de seguridad, archivos
Proceso de tratamiento de datos	Recopilación de datos de los hosts de los usuarios que utilizan el producto Safetica. Transferir los datos recopilados mediante una conexión segura a un servidor y almacenarlos en una base de datos. Se puede acceder a los datos recopilados desde la consola de Safetica y directamente desde las propias bases de datos.
Procesadores de datos externos	Se puede utilizar en caso de mantenimiento u otros servicios

	prestados por un tercero / especificar según su empresa
Transferencia de datos fuera de la UE	Puede ocurrir en caso de mantenimiento u otros servicios prestados por un tercero / especificar según su empresa
Función de la empresa (Responsable / Encargado del tratamiento)	Controlador
¿Es necesaria la EIPD?	Especifique de acuerdo con su propio procesamiento de datos
¿Perfiles?	Especifique de acuerdo con su propio procesamiento
¿Se procesa automáticamente?	Sí

Derecho a	
Acceso	Pertinente
Rectificación	Pertinente
Raspadura	Pertinente
Portabilidad	No es pertinente según la base jurídica (véase la sección correspondiente en el texto anterior)
Restringir el procesamiento	Pertinente
Seguridad aplicada	Control de acceso, configuración de SQL server, personas responsables, registros de acceso / especificar según su empresa

We have your back.



safetica