



GDPR

(Reglamento general
de protección de datos)

Conceptos fundamentales

Datos personales

Información mediante la cual una persona viva puede ser identificada

Procesamiento

Definido de forma general, es la obtención, registro o retención, o realización de cualquier operación o conjunto de operaciones

Controlador de datos

Decide los propósitos y la manera en que son procesados los datos

Procesador de datos

Procesa los datos personales en nombre del controlador de datos

Individuos de datos

Personas con las que se relacionan datos personales (incluye empleados)

Datos personales confidenciales

Subconjunto de datos personales: mayor nivel de cuidado

Notificación

Presentación ante la autoridad supervisora en caso de violación de datos personales

GDPR: principios básicos



Sanciones por incumplimiento del 4% de la facturación mundial anual o 20 millones de euros



Afecta a las empresas que procesan datos personales de individuos en la Unión Europea



Puede requerir la presencia de un Delegado de protección de datos (DPO, por sus siglas en inglés)



Notifica a las autoridades y a las personas sobre una violación dentro de estrictas líneas de tiempo



El consentimiento debe destacarse, ser claro e incluir los motivos de la recolección



Las personas pueden tomar la decisión de revocar el acceso a sus datos



Las personas tienen el derecho de obtener, cambiar, mover y borrar sus datos



Incluye protección de datos en la etapa de diseño para un nuevo sistema

A group of people holding hands in a circle, symbolizing teamwork and collaboration. The image is dimmed, with a green text box overlaid in the center. In the foreground, there is a water bottle with a black and white striped sleeve, a glass jar filled with granola, and a pen holder with several pens and markers.

Esto no se trata solo de TI

A map of North America, showing the United States and parts of Canada. The map is slightly blurred and has a dark overlay. A prominent green rounded rectangle is centered over the map, containing the text "Es a nivel mundial" in white. The map shows state and provincial boundaries, major cities, and geographical features like the Gulf of Mexico and the Atlantic Ocean.

Es a nivel mundial

5 principios básicos importantes que usted mismo puede usar para lograr el cumplimiento de GDPR

Conozca sus datos

Identifique la información de identificación personal ("PII") que su organización recopila, tiene y quién tiene acceso.

Administre sus datos

Establecer las reglas y procesos para acceder y usar PII

Proteja sus datos

Implementar y garantizar controles de seguridad para proteger la información y responder a las violaciones de datos

Documentar y cumplir

Documente sus procesos, ejecute las solicitudes de datos e informe cualquier problema o violación de datos dentro de las pautas

Mejoras continuas

Las organizaciones deben evaluar y probar constantemente sus procedimientos y protocolos existentes y evolucionar y mejorarlos a medida que nuestro mundo digital evoluciona.



1 Conozca sus datos

Lo más importante que debe tener en cuenta es que necesita conocer los datos que posee.

Identificar

Lo que debe hacer es identificar si su organización posee información de identificación personal (PII) de un residente de la UE.

PII es una categoría (muy) amplia de información. La definición es: CUALQUIER dato que pueda usarse para identificar a un individuo. Obviamente, se le ocurrirá el nombre, la información de contacto, las imágenes, pero puede ser mucho más y se puede almacenar de muchas formas. Direcciones IP, datos de ubicación a través de una aplicación, formularios de comentarios, datos de programas de recompensas y mucho más. Además de PII también hay otra categoría llamada PII sensible que tiene pautas aún más estrictas en GDPR.

Sepa también que debe mirar más allá de los datos externos. Dentro de su organización, los datos de sus empleados (principalmente con recursos humanos) también son PII y, si tiene empleados europeos, significa que también debe saber cuáles son esos datos

Acceso

Comprender quién tiene acceso a esos datos. GDPR es muy estricto sobre quién puede ver qué tipo de datos y solo las personas que necesitan acceder a él con buenas razones, que están definidas en los términos del contrato pueden tener acceso.

Elabore un mapa claro de quién tiene acceso y qué tipo de acceso tienen. ¿Pueden leerlo? ¿Todo ello? Pueden ellos modificar? Tenga en cuenta que esto debe realizarse en todas las copias de esos datos. En producción, copia de seguridad, copia de seguridad, etc.



Ubicación

También necesita saber dónde vive. Eso incluye los datos de producción, pero también cualquier copia de esos datos. GDPR solo permite la transferencia de datos a países no europeos que aplican las mismas reglas. Esta lista de países no es definitiva y puede cambiar en función de las medidas que esos países toman en torno a la privacidad de los datos.

Es probable que los datos que residen en sus propios centros de datos se encuentren fácilmente, pero ¿qué ocurre con los datos que quedan en los servicios en la nube?
¿Sabe dónde se encuentra físicamente?

A hand-drawn flowchart on a chalkboard background. The flowchart consists of several rectangular boxes connected by arrows, indicating a process flow. A hand is pointing to one of the boxes in the middle. The text is overlaid on this background.

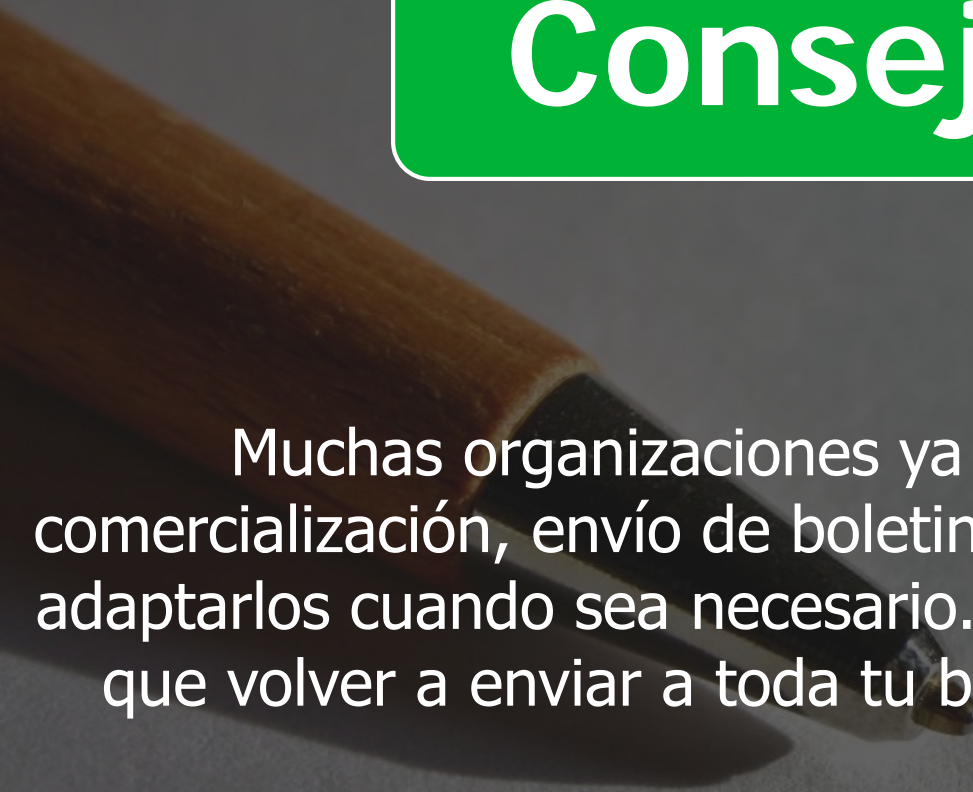
Consejo: ¡organigramas!

Crea diagramas de flujo de tus datos. Dónde se está recolectando, a qué lugar se lo está transfiriendo, qué se está haciendo con él y quién tiene acceso a él.

Un diagrama de flujo le dará una indicación visual de las respuestas a esas preguntas. Si bien es muy probable que se trate de un proceso continuo, llevará bastante tiempo la primera vez y será más fácil y consumirá menos tiempo después. Su DPO, si lo necesita, o el responsable de GDPR tendrá una vista completa del procesamiento de los datos



Consejo: ¡revisar Opt-In!



Muchas organizaciones ya tendrán acuerdos de suscripción voluntaria para comercialización, envío de boletines y mucho más. Aconsejamos revisar todos aquellos y adaptarlos cuando sea necesario. Para algunas organizaciones, eso significa que tendrás que volver a enviar a toda tu base de datos de contactos y pedir permiso de nuevo.

I Agree



2 Administre sus datos



Identificación

En la mayoría de las organizaciones, los datos PII probablemente se almacenarán en fuentes de datos específicos, como máquinas virtuales, máquinas físicas e instancias de la nube. Notamos que muchas organizaciones están usando software específico (lo más probable es que trabajen solo en datos de producción) que solo etiqueta datos específicos. Sin embargo, también es importante etiquetar a los titulares de esos datos. Si su solución de software tiene un sistema de etiquetado, úselo para etiquetar cada instancia que posee datos PII. El informe de esa solución de software debería basarse en el etiquetado, lo que hace que la vida del OPD sea más fácil de nuevo para que no tenga que extraer datos de los informes con regularidad.

¿Por qué acceder?

Durante esta fase, también es el mejor momento para revisar todas las personas o unidades de negocios que tienen acceso a cierta información. ¿Por qué tienen acceso? (Debe quedar claro a partir de esos diagramas de flujo) Hablando en un idioma de TI, este es también el momento de eliminar los nombres de usuario de las entradas de ACL y trabajar solo con grupos de seguridad. Algunas personas ciertamente tendrán acceso a datos que podrían haberse necesitado hace años pero que ya no son necesarios.

Modifíquelo, adáptelo y deje que su DPO (o su responsable asignado) revise periódicamente esas listas de acceso y retire el acceso cuando ya no lo necesite.



3 Proteja sus datos

Cifrado de extremo a extremo

Los datos son vulnerables cuando se mueven a través de la red. Si esto es interno o externo, cuando está en tránsito puede ser interceptado. También es vulnerable cuando está en REST. Esto es tanto para datos de producción como copias de esos datos. Asegúrese de utilizar cifrado de extremo a extremo para los datos.



4 Documentar y cumplir

Transferencia de datos

Cuando posee datos de una persona, esa persona puede solicitar los datos y debe entregarlos en un formato fácil. En Veeam aprendimos que la mejor manera de hacerlo es recuperar los datos de la última copia para que no interfiera con los datos de producción. Ser capaz de entrar en esas copias y exportar los datos en formatos conocidos será crucial si recibe esta solicitud. Pero si ha identificado sus datos en la lección 1, conozca la ubicación, entonces la búsqueda a través de esa copia (con las herramientas correctas) debe ser fácil y rápida.



5 Mejorar continuamente



HELP

No hay una sola solución de software o hardware que pueda cumplir. De hecho, hoy en día, ningún software puede afirmar que cumple con GDPR, ya que no existe una certificación como tal en este momento. Convertirse en GDPR compatible es un proceso que incluye flujos de trabajo, procesos, personas y software. Entonces, ¿dónde puede el software Veeam ayudar a su organización? ¿Qué informes, qué funcionalidad incluye las soluciones Veeam que ayudarán a su organización en su camino hacia GDPR?



Ubicación

Saber dónde se encuentran físicamente sus datos es importante para GDPR. En Veeam Availability Suite, hemos creado un sistema de etiquetado que le permite etiquetar sus datos de producción, copias de seguridad, copias de seguridad, réplicas e incluso ubicaciones de cintas. Hay informes disponibles que le brindan una visión general completa de dónde viven sus datos. De la producción a la cinta. Cuando desee restaurar datos en una ubicación diferente a la ubicación de producción original, se le dará una advertencia para evitar errores humanos



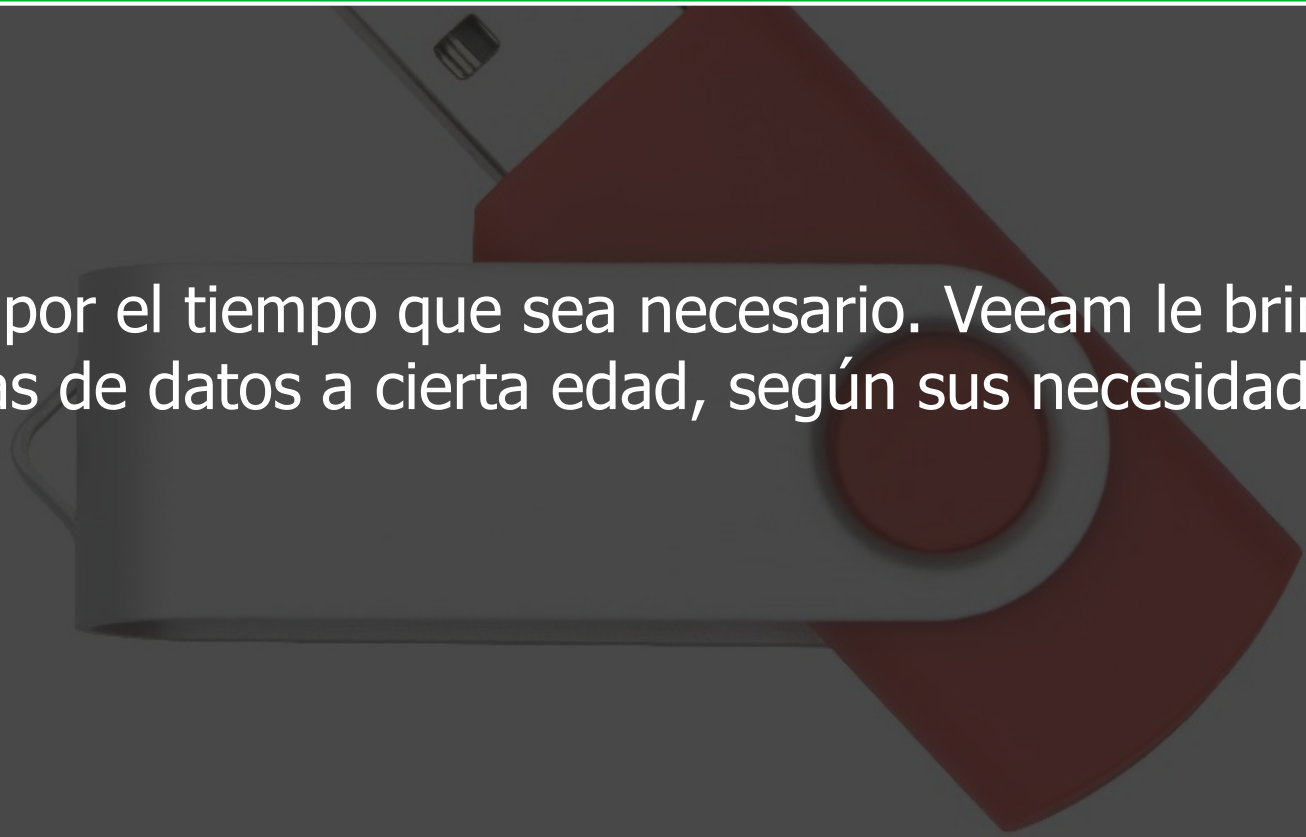
Verificación

Hablamos de protección de datos y seguridad por diseño. Y también discutimos que necesita volver a traer los datos en línea tan pronto como sea posible en caso de que algo le suceda. En Veeam, fuimos pioneros en SureBackup y SureReplica como una solución para probar si sus respaldos y réplicas son realmente utilizables en caso de un problema. A través de nuestra tecnología de laboratorio virtual, puede iniciar la máquina, ver si se ejecuta y ejecutar las secuencias de comandos dentro para probar y verificar que todo esté funcionando. Todo esto se puede hacer de forma automatizada



Retención de datos

Mantenga sus datos por el tiempo que sea necesario. Veeam le brinda la posibilidad de retirar sus copias de datos a cierta edad, según sus necesidades y requisitos.



Recuperación instantánea

Hablando de recuperaciones que necesitan ir rápido. Nuestra tecnología de recuperación instantánea, que nuevamente es algo que Veeam ha sido pionero. Iniciar la máquina desde el archivo de copia de seguridad le dará acceso instantáneo a los datos nuevamente. Al mismo tiempo, podrá transferir los datos a su ubicación original, manteniendo los datos disponibles en todo momento.

Cifrado de extremo a extremo

Veeam Software ofrece la posibilidad de encriptación de extremo a extremo tanto en tránsito como en reposo. Esto garantizará que sus datos estén seguros cuando se transfiera desde la producción a un destino de copia de seguridad o réplica, especialmente cuando abandona sus instalaciones.

Control de acceso basado en roles

(RBAC, por su siglas en inglés)

Quién tiene acceso a sus datos y, en este caso, quién tiene acceso a las copias de los datos. Con el control de acceso basado en roles de Veeam, puede definir quién tiene acceso y, mediante el informe de Veeam ONE, puede registrar las actividades e informar sobre ellas



Excluir

A veces es necesario no proteger ciertos datos debido a la sensibilidad o porque no se puede reutilizar después de un corto período de tiempo.

Veeam puede excluir datos de las copias de seguridad y réplicas basadas en máquinas virtuales, discos e incluso archivos y / o carpetas al usar nuestra tecnología de agente, manteniéndolo en conformidad en todo momento

¡Gracias!

VEEAM