NUEVO RGPD

TODO LO QUE NECESITA DE SABER SOBRE LA NUEVA LEY DE PROTECCIÓN DE DATOS

datapeers

ÍNDICE

Contexto 3

La necesidad de proteger la información 4

Una breve mirada sobre el nuevo reglamento 5

El nuevo reglamento 7

¿El RGPD se aplica a su organización? 9

¿El RGPD se aplica a su organización? - casos prácticos 10

El precio de la infracción 11

Checklist del nuevo reglamento 12

¿Que puedo hacer? 15

La solución Datapeers 16

La solución Datapeers - características 17

la solución Datapeers - aspectos técnicos 18

La solución Datapeers - esquema de funcionamento 19

Retorno sobre la inversión garantizada 20

Preguntas frecuentes 21

CONTEXTO

Las empresas se enfrentan a amenazas crecientes de seguridad y confidencialidad de los datos, lo que les obliga a reevaluar sus estrategias de gestión de datos. Todos nosotros en algún momento de nuestra vida realizamos acciones online, como comprar un producto, suscribir un servicio o efectuar una transferencia bancaria. Las nuevas tecnologías potencian un gran número de oportunidades en la optimización de los recursos, pero cuando son mal utilizadas pueden comprometer la seguridad de la información de los ciudadanos.

Una de las mayores preocupaciones de todas las empresas es la protección de la información. Nunca antes como ahora la necesidad de proteger los datos fue tan evidente. Un estudio llevado a cabo por Forrester prevé que el número global de usuarios de smartphones supere los 3.500 millones en 2020 y este uso masivo de dispositivos móviles potencia la existencia de ataques informáticos, comprometiendo a gran escala la privacidad de todos y de cada uno uno.

Los ciudadanos deben tener control sobre los datos personales y debe simplificarse el marco legal de los negocios digitales. Para la Comisión Europea, la protección de los datos personales es un elemento clave del Mercado Único Digital. Todo este escenario potenció la creación del nuevo Reglamento General de Protección de Datos (RGPD) para la Unión Europea, que deroga la legislación actual sobre la protección de los datos personales, publicada en 1995, cuando el acceso a Internet aún no era generalizado.
El nuevo Reglamento entrará en vigor en mayo de 2018.

LA NECESIDAD DE PROTEGER LA INFORMACIÓN

78%

de las empresas en todo el mundo sufrió al menos un ataque informático en los últimos dos años

92%

de los ataques sufridos ocurre debido a fallas de seguridad internas

35%

de los ataques sufridos ocurre debido a pérdidas de información en dispositivos móviles

57%

de las empresas no protege su información con soluciones de protección de datos

61%

de pérdida de productividad en cada ataque informático

42%

de pérdida de ingresos en cada ataque informático

3%

de las empresas tiene un plan en curso para garantizar el cumplimiento con el RGPD en mayo de 2018

4,8%

de las empresas conoce bien el nuevo reglamento de protección de datos

44%

de las empresas admite que no tiene ningún plan para ajustarse al RGPD en la fecha de su entrada en vigor

datapeers

UNA BREVE MIRADA SOBRE EL NUEVO REGLAMENTO

Nombre oficial

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de dichos datos

Plazo

Entra en vigor el 25 de mayo de 2018

Propósito

Da a los individuos en la Unión Europea derechos más fuertes, dotándolos de mayor control sobre sus datos y privacidad en la era digital

UNA BREVE MIRADA SOBRE EL NUEVO REGLAMENTO

¿Qué son datos personales?

De acuerdo con la legislación, se consideran datos personales cualquier información relativa a una persona individual identificada o identificable a través de los mismos (identificable «por referencia a un número de identificación o a uno o más elementos específicos de su identidad física, fisiológica, psíquica, económica, cultural o social »)

Certificación

Existe una certificación opcional para las empresas que cumplan con éxito los requisitos legales. Esta certificación puede significar una ventaja competitiva y ayudar a construir confianza de los clientes

EL NUEVO REGLAMENTO

El proceso legislativo sobre el nuevo Reglamento se inició en 2012 en la Comisión Europea y tras algunos debates llegó a la versión final que se publicó a principios de mayo de 2016. Esta nueva ley se aplica a los 28 Estados-miembros de la Unión Europea y entra en vigor con carácter obligatorio, el 25 de mayo de 2018.

Los cambios más significativos e impactantes de este nuevo Reglamento son los siguientes:

- **Derecho al olvido:** los ciudadanos podrán exigir a las empresas que eliminen los datos personales. Este derecho al olvido es una prolongación del derecho ya existente de impedir que los datos personales sean tratados. El nuevo reglamento permite que los datos personales de cada ciudadano sean destruidos por su solicitud.

- **Portabilidad de los datos:** los ciudadanos podrán exigir a las empresas que les envíen sus datos personales en un formato que permita que sean enviados a otra empresa, facilitando su migración y haciendo más simple el cambio de prestación de servicios. Siempre que un ciudadano cambie de Banco o de prestador de servicios de televisión, no tendrá que proporcionar nuevamente sus datos personales, ya que éstos pueden migrar fácilmente de una empresa a otra.

EL NUEVO REGLAMENTO

- **Derecho de oposición al profiling:** los sistemas informáticos de las empresas deberán poder registrar quién indicó la negativa al tratamiento automatizado de sus datos, como se suele hacer en procesos de análisis conductuales y creación de perfiles de consumo. En estas situaciones, los registros no podrán incluirse en los procesos.

- **Registros y prueba de consentimiento:** En la relación en línea con los clientes, los sistemas de las empresas deben exponer las políticas de privacidad en un lenguaje claro y objetivo. El consentimiento del tratamiento de los datos por parte de los ciudadanos deberá guardarse para servir como prueba de consentimiento libre e inequívoco.

- **Privacidad por defecto y diseño:** se deben tomar medidas que aseguren la protección de los datos desde el diseño de aplicaciones informáticas, minimización del tratamiento de datos personales, enmascaramiento de los datos, encriptación, entre otros aspectos. El objetivo es lograr explicar todo el proceso de tratamiento y protección de los datos.

- **Obligatoriedad de notificar:** las empresas y las organizaciones tienen la obligación de notificar a la Autoridad Nacional de Dupervisión para las infracciones de datos para situaciones que pongan a las personas en riesgo y comunicarse al ciudadano de que se trate todas las infracciones de alto riesgo lo antes posible, de modo que puedan adoptarse las medidas apropiadas.

¿El RGPD SE APLICA A SU ORGANIZACIÓN?

La nueva ley de protección de datos se aplica a cualquier organización que haga negocios en la Unión Europea, independientemente de que el procesamiento de los datos personales se produzca en la Unión Europea o no, y con independencia de que sean datos personales sobre residentes de la Unión Europea o sólo visitantes.

Es importante subrayar que las nuevas normas se aplican a las empresas establecidas fuera de la Unión Europea que procesan datos personales de residentes o visitantes de la Unión Europea en relación con:

- Las ofertas de bienes o servicios, independientemente de si se requiere el pago, o;
- Supervisión del comportamiento que se produce en la UE.

Tener un sitio web o un e-mail accesible en la Unión Europea no es suficiente para poner el negocio bajo la alzada del nuevo reglamento de protección de datos. Sin embargo, algunos factores pueden indicar que una organización pretende ofrecer bienes o servicios a residentes o visitantes en la Unión Europea, que traen el negocio al ámbito de las nuevas reglas. Estos factores son:

- El uso de una lengua o una moneda generalmente utilizada en uno o varios Estados-miembros de la Unión Europea con la posibilidad de encargar mercancías y servicios en ese idioma;
- La mención de clientes o usuarios que se encuentren en la Unión Europea.

¿El RGPD SE APLICA A SU ORGANIZACION? Casos prácticos

Escenario 1

Una empresa con sede en Nueva York tiene la función de proyectar los beneficios de una empresa alemana para los próximos tres años. Los empleados de la empresa estadounidense utilizarán datos proporcionados por la empresa alemana. Por lo tanto, la empresa estadounidense está obligada a cumplir las nuevas normas del RGPD, porque los datos se recogieron en el territorio de la Unión Europea.

Escenario 2

"BuyEverything" es un sitio web americano que permite comprar varios productos en línea. El sitio recoge datos que posteriormente utiliza en campañas de marketing. Si una persona visita el sitio web en territorio de la Unión Europea, el sitio se convierte en "objeto" de la nueva ley. Esto significa que cualquier sitio web que recoja datos y que permita visitas procedentes de la Unión Europea está obligado a cumplir el nuevo RGPD.

EL PRECIO DE LA INFRACCIÓN

Las infracciones para las empresas que no cumplen la nueva ley de protección de datos son bastante pesadas y son un importante incentivo para que la ley se cumpla en toda su plenitud.

No se ha definido el valor mínimo para las multas, pero las multas por incumplimiento de datos personales pueden alcanzar los 20 millones de euros o hasta el cuatro por ciento del volumen anual de negocios de la empresa a nivel mundial.

Las multas pueden llegar a los €20.000.000,00 o, en el caso de una empresa, hasta el 4% de su volumen de negocios anual a nivel mundial correspondiente al ejercicio financiero anterior, según el importe más elevado.

CHECKLIST DEL NUEVO REGLAMENTO

Inventario de datos personales

Haga una lista de todos los datos personales que contiene con información detallada sobre la ubicación de almacenamiento. Así será más fácil tener un entendimiento exhaustivo sobre la forma en que los datos personales se almacenan en su empresa.

Análisis del flujo de datos

Identifique todos los sistemas que almacenan datos personales bajo el nuevo RGPD. Debe asignar los flujos de datos desde su punto de entrada hasta el momento de la destrucción, incluindo los procesos de terceros. Esta asignación de datos le ayudará a garantizar que todos los riesgos de pérdida de datos personales se eliminan (o son ampliamente minimizados).

CHECKLIST DEL NUEVO REGLAMENTO

Registro de las actividades de tratamiento

Debe registrar detalladamente todas las actividades relacionadas con el tratamiento de datos personales, de modo que la organización demuestre que cumple todas las obligaciones en vigor en el RGPD. La legislación prevé que las entidades en régimen de subcontratación tengan casi las mismas obligaciones que los responsables del tratamiento, por lo que deben demostrar que cumplen lo exigido.

Identificación de lagunas

Defina cómo va a corregir las lagunas detectadas durante el período de evaluación del riesgo. Priorice los problemas de acuerdo con el riesgo que presentan. El plan de acción para estas situaciones puede incluir: contratación de nuevos colaboradores, formación de colaboradores actuales, cambios de procesos y métodos e implementación de nuevas tecnologías.

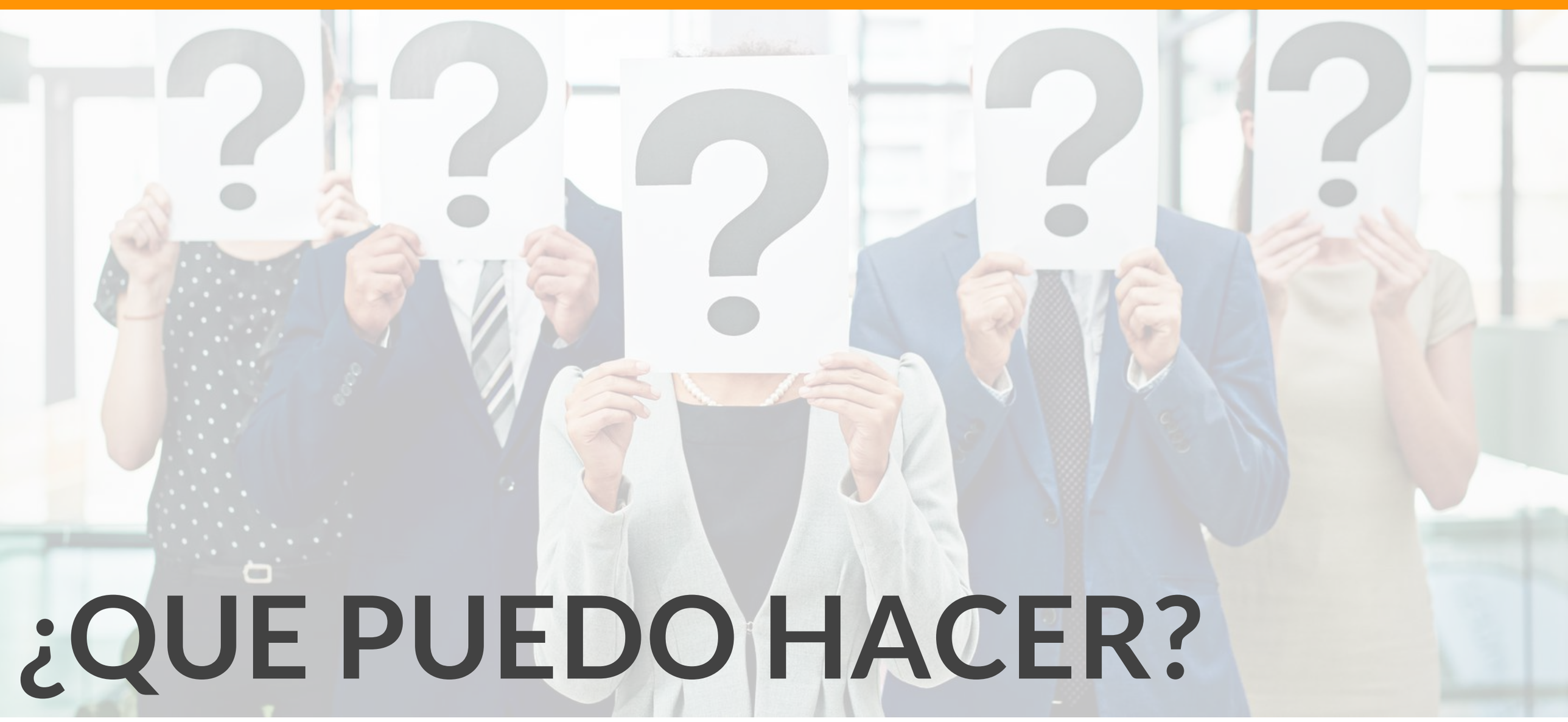
CHECKLIST DEL NUEVO REGLAMENTO

Evaluación de riesgos

Siga los puntos de contacto para los datos y realice una evaluación de riesgo para cada fuente de datos y ubicación de almacenamiento. De esta forma, va a estar más preparado en caso de ataque y será capaz de identificar y minimizar los riesgos de sufrir algún ataque y perder datos.

Nombramiento de un Encargado de Protección de Datos

Esta figura desempeña un papel esencial en el período de transición de la ley antigua a la nueva legislación. La persona responsable de la protección de datos debe asegurarse de que todo se encuentra perfectamente legal en la fecha de entrada en vigor del RGPD.



¿QUE PUEDO HACER?

Analizar los datos personales gestionados por la organización
- hacer un inventario sobre estos datos: tipo de datos, donde fueron recogidos y donde están almacenados.

Verificar la política de privacidad para los datos recopilados
- verificar si las políticas de privacidad existentes en la organización son claras y explícitas, promoviendo la fácil comprensión por parte de los usuarios

Nombrar un Data Protection Officer
- obligatorio para empresas con más de 250 trabajadores o para empresas que tengan en su core business el procesamiento de datos de terceros o que trate de datos de categorías especiales (racial, étnica, política, religiosa, entre otras).

Implementar políticas de gestión y protección de datos
-Garantir que se conoce la localización de los datos personales, que éstos se encuentran debidamente protegidos de acceso no autorizado o enmascarado y que son fácilmente eliminados si hay solicitud.

*** Contamos con un equipo profesional capaz de ayudarle en esta fase de transición al nuevo RGPD. Hable con nosotros en caso de duda.**

LA SOLUCIÓN DATAPEERS

INTEGRIDAD DE DATOS

GESTIÓN DE DATOS DE PRUEBA

SUBCONJUNTOS DE DATOS

ENMASCARAMIENTO DE DATOS

INTEROPERABILIDAD

Datapeers es una solución innovadora y automatizada que permite el enmascaramiento de datos y ayuda a las empresas a cumplir los requisitos de privacidad de los datos y al mismo tiempo aumenta la calidad de los procesos de desarrollo, pruebas, formación y certificación de software.

Datapeers es una solución completa que permite la creación automatizada de bases de datos no productivas basadas en subconjuntos de datos de producción. De este modo, permite que se generen datos de prueba que cumplan los estándares más exigentes de las pruebas de software.

LA SOLUCIÓN DATAPEERS
Características



✓ Técnicas de enmascaramiento sofisticadas para proteger datos sensibles

✓ Detección automática de dependencias de datos y relaciones ocultas

✓ Extracción inteligente de subconjuntos de datos y creación de datos relevantes para diferentes ambientes

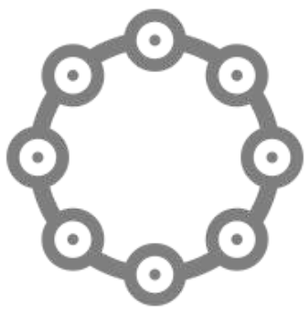
✓ Cumple las normas de protección de datos confidenciales como el PCI-DSS y el RGPD

datapeers

LA SOLUCIÓN DATAPEERS
Aspetos técnicos

INTEGRIDAD REFERENCIAL
Relación entre datos coherentes, garantizando la calidad de los datos incluso después de los cambios

MASCARAMIENTO DE LOS DATOS
Sustitución de datos reales por datos ficticios pero realistas, de acuerdo con las principales reglas y reglamentos de protección de datos corporativos y gubernamentales



INTEROPERABILIDAD
Posibilidad de trabajar con múltiples tecnologías de bases de datos y sistemas operativos

GENERACIÓN DE DATOS DE PRUEBA
Generador de datos que permite a los programadores y administradores llenar bases de datos automáticamente con datos de prueba significativos y realistas

SUBCONJUNTOS DE DATOS
Varios subconjuntos de datos que reflejan con precisión la base de datos de producción original y atiende a las necesidades específicas de cada tipo de prueba

LA SOLUCIÓN DATAPEERS

Esquema de funcionamento

RETORNO SOBRE LA INVERSIÓN GARANTIZADA

✓ **Aumenta hasta un 80% la productividad** de los equipos al automatizar la mayoría de las tareas de gestión de datos de prueba

✓ **Reduce los costos de las pruebas** hasta el 75%

✓ **El tiempo de prueba** de nuevos entornos **se reduce a la mitad**

✓ El aumento de la calidad de los datos **disminuye la necesidad de repetir pruebas hasta obtener la calidad deseada**

✓ **Reduce los costos de infraestructura** mediante la optimización de los recursos de disco y servidor

✓ **El retorno de la inversión se alcanza en menos de seis meses** después de la implementación del Datapeers

✓ Garantiza que los ambientes no productivos cumplen con las obligaciones derivadas del RGPD

PREGUNTAS FRECUENTES

¿Es necesario obtener el consentimiento del titular de los datos en el caso de una base de datos con información de dominio público (por ejemplo: número de orden profesional en el sector de la Salud)?
Esta cuestión es un paradigma, pues los datos relacionados con el sector de la salud son sensibles y se recomienda el acceso sólo a los datos estrictamente necesarios para la prosecución de la función del colaborador. En estas situaciones, para mantener la confidencialidad e integridad de los datos, se aconseja el uso de una herramienta de enmascaramiento de datos, como el Datapeers.

¿Qué es la Evaluación de Impacto sobre la protección de datos (DPIA)?
De acuerdo con la Comisión Europea, el DPIA (Data Privacy Impact Assessment, es decir, Evaluación de Impacto de la Privacidad de Datos) es un proceso destinado a describir el procesamiento de datos privados, que evalúa la necesidad de un procesamiento y que ayuda a gestionar los riesgos relacionados con el tratamiento de datos personales. Es una evaluación de riesgo, que relaciona el impacto de las amenazas de privacidad de datos con su probabilidad de ocurrir.

PREGUNTAS FRECUENTES

¿Cuáles son los principales cambios en cuanto al consentimiento de los individuos y las empresas?

El reglamento crea barreras adicionales a las prácticas actuales de recogida y tratamiento de datos en Portugal, introduciendo reglas más estrictas a las empresas en lo que se refiere al consentimiento para la recogida y tratamiento de datos personales. Las empresas tienen que considerar la creación de un contrato con el titular de los datos, el cumplimiento de obligaciones jurídicas y la defensa de intereses vitales del titular de los datos. Con el nuevo reglamento, un contacto de una tarjeta de visita, por ejemplo, no podrá ser incluido en ninguna base de datos sin el consentimiento explícito de su titular. En términos prácticos, el uso de cajas previamente seleccionadas, la ausencia de respuestas, la inactividad y el consentimiento a través de términos y condiciones dejarán de ser permitidos, pues ninguno de los medios presentados es considerado un medio de demostración del cumplimiento de los requisitos de consentimiento del nuevo Reglamento.

Hable con nosotros y sepa cómo podemos ayudarle a vencer los desafíos del nuevo RGPD

PARA MÁS INFORMACIONES:

Centro Empresarial da Maia
Rua Eng. Frederico Ulrich, 3210
4470-605 Maia, Portugal

www.datapeers.itpeers.com
datapeers.info@itpeers.com
+351 220 101 587

datapeers