Informatica

White paper

Recomendaciones para afrontar todo lo relacionado con los datos de este reglamento

ACERCA DE INFORMATICA

La transformación digital modifica las expectativas: mejor servicio, entrega más rápida, menores costes. Los negocios deben transformarse para seguir siendo relevantes y los datos tienen la respuesta.

Como líder mundial en gestión de datos de cloud empresariales, le brindamos ayuda para que encabece la marcha de forma inteligente, en cualquier sector, categoría o nicho. Informatica le aporta perspectiva para que aumente su agilidad, concrete nuevas oportunidades de crecimiento o incluso invente cosas nuevas. Al estar completamente centrados en todo lo relacionado con los datos, ofrecemos la versatilidad necesaria para alcanzar el éxito.

Le invitamos a explorar todo lo que puede ofrecerle Informatica y a desatar el poder de los datos para impulsar su próxima disrupción inteligente.

Contenidos

1. Resumen ejecutivo

A partir de mayo de 2018, el reglamento general de privacidad de datos de la Unión Europea entra en vigor, lo que permite una mayor protección de los datos personales. El reglamento general de privacidad de datos se aplica a cualquier organización establecida en la UE y a cualquier organización (en cualquier parte del mundo) que procesa los datos personales de los usuarios de datos de la UE al ofrecerles bienes o servicios, o al supervisar o realizar un seguimiento de sus actividades. Este reglamento podría afectar considerablemente a muchas organizaciones y al modo en que gestionan los datos relativos a los clientes, consumidores, socios, empleados y otros "usuarios de datos"; donde un "usuario de datos" es una persona. El reglamento general de privacidad de datos afecta al almacenamiento, procesamiento, acceso, transferencia y divulgación de los registros de datos de una persona, además de tener algunas sanciones potencialmente cuantiosas por vulneraciones.

El reglamento general de privacidad de datos requerirá que muchas organizaciones comprendan plenamente cómo utilizan los activos de información actuales y futuros para incorporar estos nuevos requisitos en materia de privacidad de datos y mejorar los derechos de privacidad de los ciudadanos. Para muchos, los cambios asociados a las prácticas de gestión de la información requerirán una evaluación exhaustiva de las funcionalidades de los datos actuales y futuros. Este documento explora cómo eliminar estos requisitos ayuda a la comprensión de los desafíos que plantean los datos y la dirección que las organizaciones podrían tomar con respecto a sus iniciativas en relación con el reglamento general de privacidad de datos.

Para facilitar la comprensión, en este documento se analizan algunas de las preguntas más comunes que muchas organizaciones formulan sobre su transición al reglamento general de privacidad de datos. Nosotros las llamamos preguntas relativas a los puntos de entrada. Para ayudar a contestar cada pregunta relativa a los puntos de entrada, hemos establecido un conjunto de requisitos de funcionalidades que consideramos importantes y, en consonancia con cada funcionalidad, hay un caso de uso de tecnología para el modo en que se puede desarrollar cada funcionalidad. La tabla que aparece a continuación muestra cómo están relacionados todos estos elementos.

Pregunta relativa a los puntos de entrada	Requisito de funcionalidad	Caso de uso de tecnología
¿Dónde están todos nuestros datos dentro del alcance potenciales?	Detección de datos sensibles y análisis de riesgos	Detección y protección
¿Cómo se están utilizando nuestros datos personales?	Interpretación de políticas	Gobierno de datos empresariales
¿Cómo gestionamos los datos de los usuarios de datos?	Gestión de datos personales	Caso de uso de correspondencia y vinculación de datos
¿Cómo podemos proteger los datos y evitar el acceso no autorizado?	Habilitación de controles de seguridad de datos	Detección y protección

También hay ejemplos donde los requisitos, tales como el consentimiento para la captura y la gestión, pueden abarcar múltiples requisitos de funcionalidades y casos de uso de tecnología; por lo tanto, las organizaciones deben tener una plena comprensión de las posibles complejidades involucradas.

Aunque el reglamento general de privacidad de datos plantea muchos desafíos, ofrece numerosas oportunidades en torno al uso de los datos. Este documento describe los posibles enfoques de casos de uso y se basa en nuestra amplia experiencia en la gestión de datos para ayudar a las organizaciones a abordar simultáneamente estos desafíos e introducir funciones innovadoras de gestión, gobierno y seguridad de datos para maximizar sus programas de cumplimiento. Informatica ofrece soluciones de software integradas e innovadoras para automatizar, proteger y controlar los datos, y estas soluciones pueden ayudar rápidamente a las organizaciones en sus iniciativas relacionadas con el reglamento general de privacidad de datos.

2. Background

2.1 Información general y posibles consecuencias

La digitalización de la sociedad avanza a un ritmo rápido, ya que casi todas las organizaciones aprovechan el poder de los datos para mejorar las decisiones de negocios, atraer a los clientes y socios, e impulsar procesos de negocio transformativos. La Comisión Europea ha reconocido que gran parte de los datos que se crean, recopilan, procesan y almacenan son, en realidad, datos personales, que pueden revelar una amplia información de los usuarios de datos de la UE.

Los reglamentos de protección de datos existentes no han reducido necesariamente las preocupaciones relativas a la protección y la seguridad de los datos personales. La diversidad de reglamentos de protección de datos de los estados miembros de la UE frustra a los usuarios de los datos, ya que un 90 % indican que les gustaría los mismos reglamentos de protección de datos en toda la UE, independientemente del lugar donde se almacenan o procesan sus datos.*

Por lo tanto, el reglamento general de privacidad de datos se ha establecido para proteger mejor los derechos fundamentales de privacidad de los ciudadanos en la era digital, así como para abordar las preocupaciones sobre la diversidad de las leyes de protección de datos.

A partir de mayo de 2018, el reglamento general de privacidad de datos requerirá que muchas organizaciones gestionen y protejan de manera más eficaz los datos sobre clientes, ciudadanos y empleados, entre otros. Este reglamento se aplica a los usuarios de datos de la UE, independientemente de su nacionalidad o residencia, a fin de proporcionar principios y normas sobre la protección de datos personales.

Dado que el reglamento general de privacidad de datos es un reglamento basado en “principios”, esto implica que las organizaciones deben plantearse qué obligaciones pueden o no tener que cumplir, dadas las circunstancias excepcionales de su negocio y su uso de los datos. Por lo tanto, muchas organizaciones tendrán que crear una interpretación de estos principios para ayudar a guiar y orientar sus iniciativas relacionadas con el reglamento general de privacidad de datos.

El reglamento general de privacidad de datos requerirá que muchas organizaciones comprendan mejor cómo van a utilizar sus activos de información actuales y futuros para cumplir estos nuevos principios de privacidad de datos. Esto afectará a las personas, los procesos, la tecnología y las prácticas y políticas de gestión de datos de muchas organizaciones.

Las vulneraciones del reglamento podrían conllevar importantes sanciones económicas para muchas organizaciones, en función del tipo y la magnitud de la vulneración. Se podrían aplicar multas de hasta 20 millones de euros o el 4 % de la facturación anual total a nivel mundial de una organización, lo que sea mayor.

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.2 ¿A quién concierne el reglamento general de privacidad de datos?

El cumplimiento del reglamento general de privacidad de datos tiene múltiples dimensiones y no está limitado por la geografía física; las organizaciones de Norteamérica y Asia, entre otras, deben cumplirlo si almacenan y procesan usuarios de datos de la UE. En la actualidad, las organizaciones que tratan directamente con los consumidores (B2C) y las organizaciones que trabajan con otras organizaciones (B2B), así como las empresas de procesamiento de datos específico, manejan datos personales.
Las organizaciones que procesan datos sobre usuarios de datos de la UE tendrán que comprender plenamente sus requisitos de cumplimiento, independientemente del país en el que se ubiquen físicamente sus centros de operaciones o de datos.

2.3 ¿Qué hace complicado el reglamento general de privacidad de datos desde el punto de vista de los datos?

Para muchas organizaciones, los datos plantean distintos desafíos en relación con el reglamento general de privacidad de datos. El cumplimiento del reglamento general de privacidad de datos implica el control y el gobierno de los datos personales, dondequiera que se encuentren dentro de una organización. Sin embargo, la proliferación de datos en toda la organización y sus ecosistemas empresariales pueden hacer que la gestión de los datos sea complicada. Las tendencias más significativas, como el aumento de la diversidad de datos y la transición a los entornos informáticos basados en cloud, se añaden a los desafíos de la gestión y la seguridad de los datos al crear un entorno de TI muy dinámico. Para demostrar estos desafíos, hemos proporcionado algunas preguntas que muchas organizaciones intentan contestar en relación al reglamento general de privacidad de datos:

- ¿En qué lugar de cualquier organización, y de su ecosistema, se encuentran todos los datos pertinentes y dentro del alcance a los que se aplicarían los principios del reglamento general de privacidad de datos? ¿Están expuestos a riesgos esos datos?
- ¿Cómo mantienen las organizaciones un seguimiento de sus datos en todos sus ecosistemas operativos?
- ¿Cómo puede una organización definir y gestionar todos sus activos de datos pertinentes para ayudar a garantizar el cumplimiento y la aplicación de todas las políticas y procedimientos necesarios?
- ¿En qué lugar de cualquier organización se conservan todos los registros de datos pertinentes y dentro del alcance a los que se aplicarían los principios del reglamento general de privacidad de datos? ¿Cómo se pueden identificar y vincular?
- ¿Cómo puede una organización capturar y gestionar el consentimiento proporcionado por un usuario de datos? ¿Cómo puede una organización gestionar los cambios en la elección del consentimiento del usuario de datos o gestionar la definición del consentimiento?
- ¿Cómo puede una organización responder de forma eficaz y eficiente a las solicitudes de acceso, el derecho de borrado y las solicitudes de portabilidad de los usuarios dentro de los plazos exigidos?
- ¿Cómo controla la organización el acceso a los datos pertinentes? ¿Los datos relacionados con privacidad se eliminan cuando no son necesarios para la función o la actividad de la organización?

2.4 Tipos de datos potencialmente dentro del alcance

Otro problema potencial es cómo responden las organizaciones a los tipos de datos que conservan. En este contexto, definimos los tipos de dos maneras:

1. Un tipo de entidad de datos
2. Un tipo de tecnología que gestiona el tipo de entidad de datos

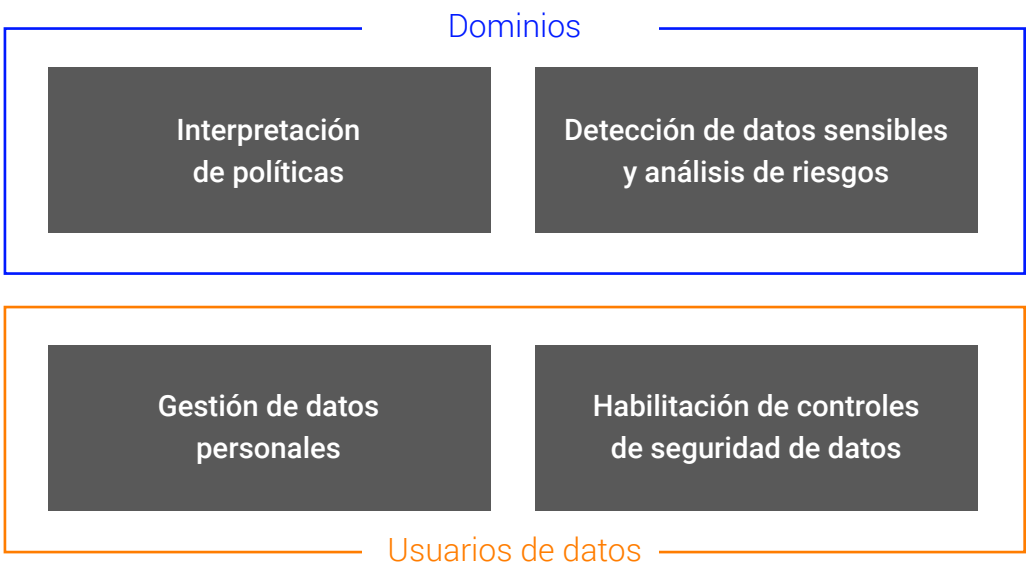
La mayoría de los fragmentos de información del usuario de datos encajarían en uno o varios tipos de entidades de datos, así como en uno o varios tipos de tecnología. En el diagrama siguiente se muestran algunos ejemplos de posibles tipos de datos y tecnología, que pueden aplicarse a los datos dentro del alcance en relación con el reglamento general de privacidad de datos:

ENTIDAD DE DATOS	TECNOLOGÍA				
• Cliente • Cliente • Titular de póliza • Beneficiario • Contacto • Empleado • Contratista • Voluntario • Visitante • Otro	• Estructurados • Semiestruc-turados • No estructu-rados	• En línea • Near line • Offline • Copia de seguridad	• Digital • Físicos • Combinados	• Explícitos • Implícitos • Combinados	• A nivel interno • Externo

Estos tipos diferentes pueden requerir que las organizaciones se planteen enfoques, métodos y tecnologías muy diferentes para la captura y la gestión de activos de datos dentro del alcance en relación con el reglamento general de privacidad de datos.

3. Puntos de entrada, requisitos de funcionalidades y casos de uso de tecnología

Para ayudar a impulsar la comprensión y el conocimiento, así como a facilitar la planificación de actividades, Informatica ha identificado a varias preguntas relativas a los puntos de entrada fundamentales que destacan algunos de los desafíos más comunes que plantean los datos del reglamento general de privacidad de datos. Estos puntos de entrada a menudo se basan en preguntas sencillas que pueden exigir a las organizaciones que reflexionen sobre las personas, los procesos y la tecnología que necesitan para crear las respuestas. Para ayudar a responder a estas preguntas, hemos descrito las funcionalidades posibles que se necesitan, así como algunos casos de uso de tecnología que ofrecen las funcionalidades necesarias. Las capacidades necesarias están estructuradas en grupos; el diagrama a continuación muestra cómo funciona el agrupamiento y la pertinencia de cada grupo.



Estas funcionalidades se sitúan dentro de dos áreas denominadas dominios y usuarios de datos.

Dominios está relacionado con los dominios de los datos del usuario de datos. Ayuda a proporcionar información sobre la detección y la gestión de los dominios, que se utiliza al definir el ámbito y al proporcionar una visión organizativa de los datos.

Usuarios de datos está relacionado con los datos reales del usuario de datos en un nivel transaccional. Ayuda a proporcionar información sobre la gestión de datos personales, que se utiliza para proporcionar respuestas a nivel de usuario e información a nivel de usuario.

3.1 Pregunta relativa a los puntos de entrada: ¿Dónde están todos nuestros datos dentro del alcance potenciales?

Contexto: Los datos suelen estar repartidos en numerosos sistemas, aplicaciones y fuentes en una empresa, sobre todo en las grandes organizaciones y en aquellas que han crecido gracias a una adquisición. Debido a las funciones que los usuarios de datos de la UE podrían desempeñar en una organización (cliente, proveedor, socio, empleado, etc.), es poco probable que los datos personales se limiten a un departamento o sistema. Las organizaciones con una mayor variedad de sistemas de TI no solo deben tener en cuenta los datos de las aplicaciones principales, sino también de las hojas de cálculo, las bases de datos locales y las soluciones de Big Data.

Funcionalidades necesarias: La detección de datos sensibles y el análisis de riesgos son funcionalidades para detectar datos en una amplia variedad de soluciones tecnológicas, y se utilizan, junto con otras fuentes de información, como las cantidades de datos reales y la proliferación de datos, para crear una puntuación de riesgo para los datos. La puntuación de riesgo ayuda a las organizaciones a comprender dónde se almacenan los datos que corren más riesgo, de manera que se puede dar prioridad a cualquier posible corrección o requisito de control de seguridad en función de un riesgo. El seguimiento de la puntuación de riesgo a lo largo del tiempo muestra si las actividades de corrección o control han mejorado la situación de riesgo de los datos. Para apoyar los fines lícitos, puede ser necesario el consentimiento para que las funciones, como el linaje de datos, ayuden a las organizaciones a identificar nuevos almacenes de datos personales a fin de facilitar la comprensión de los cambios potenciales en el uso.

Caso de uso de tecnología: La detección de datos sensibles y el análisis de riesgos podrían caracterizarse como un caso de uso de detección y protección, con especial atención a la parte de la detección. Estas son las funcionalidades principales para proporcionar información sobre dónde se encuentran los datos sensibles dentro del alcance y hacia dónde proliferan, con información analítica sobre el riesgo para los datos. Entre las funcionalidades típicas que se podrían aplicar a este caso de uso se encuentran:

- **Definición de política de datos:** definiciones de empresa y TI, datos imprecisos, conflictos de políticas
- **Detección de datos automatizada:** encontrar datos sensibles dentro del alcance relevantes, supervisión inicial además de continua, clasificación de datos, respaldo de la integración de sistemas
- **Proliferación de datos:** ¿Dónde están los datos? ¿Dónde van? ¿Nuevas fuentes?
- **Puntuación de riesgos de datos:** basada en la transferencia de los datos, la proliferación, el acceso y el volumen, la priorización más la planificación, el historial y la supervisión de la puntuación con el tiempo
- **Protección de datos:** identificar dónde necesita restricciones el acceso a los datos, qué datos se deben seudonomizar, dónde se debería aplicar el cifrado y la visualización de los datos en función del tiempo, la ubicación y la función

Soluciones tecnológicas: podría utilizarse **Informatica Secure@Source** para ayudar a detectar las ubicaciones de los datos dentro del alcance, a clasificar los datos, a supervisar la proliferación de datos y a asignar las puntuaciones de riesgo. El seguimiento a lo largo del tiempo muestra cómo influyen de forma positiva o negativa estos cambios en los esfuerzos en materia de cumplimiento.

Ventaja: no solo proporcionar información sobre la ubicación de los datos, sino también clasificar los datos según el riesgo.

3.2 Pregunta relativa a los puntos de entrada: ¿Cómo se están utilizando nuestros datos personales?
Contexto: nuestro mundo está experimentando una transformación digital que afecta a todos los sectores. El aumento de los datos generados, recopilados y analizados es una clara tendencia mundial, y un porcentaje considerable de estos datos se puede atribuir a los datos personales de los individuos. A medida que los datos proliferan en una organización, la propiedad, el control y la gestión de estos datos se vuelven más difíciles. Como muchas formas de cumplimiento de las normativas, el cumplimiento del reglamento general de privacidad de datos se alcanzará de forma óptima a través de un enfoque del gobierno de datos que abarque toda la empresa.

Funcionalidades necesarias: la interpretación de políticas es una funcionalidad para captar la comprensión empresarial y tecnológica de políticas, responsabilidades, procesos, términos de datos y modelos lógicos y físicos. Y, aún más importante, también es el lugar donde la comprensión del entorno técnico está vinculada a la comprensión del entorno empresarial. Esta vinculación proporciona a las organizaciones una visión global de la información sobre sus dominios de datos dentro del alcance y forma una parte integral de un enfoque de la gestión de sus activos de datos.

Caso de uso de tecnología: la interpretación de políticas podría caracterizarse como un caso de uso de gobierno de datos empresariales. Estas son las funcionalidades principales para proporcionar una visión ascendente y descendente de la gestión organizativa de los datos, con vínculos entre la visión de la información de la empresa y de TI. Entre los requisitos típicos que se aplicarían a este caso de uso se encuentran:

- **Definición de políticas:** definiciones de empresa y TI, documentación en todos los niveles operativos de la empresa, datos lógicos y físicos y modelos de proceso
- **Responsabilidades:** ¿quién es el propietario de los datos, quién utiliza los datos y qué funciones son responsables de la calidad y la seguridad?
- **Definición de términos y procesos:** proceso de negocio, entidades de datos clave, atributos, sistemas, calidad y controles, estandarización, definiciones del consentimiento de la empresa
- **Proceso de cambio:** proceso gobernado para las definiciones, proceso gobernado para el cambio, gobierno de procesos
- **Vinculación con artefactos:** Vinculación con artefactos de lógicos a físicos, linaje de datos técnicos y de negocio, incorporación de la calidad de datos

Soluciones tecnológicas: adoptar soluciones de gobierno de datos empresariales que permiten a las funciones empresariales y de TI trabajar conjuntamente por la meta común del gobierno de datos. Soluciones, como la del **gobierno de datos Informatica Axon**, están diseñadas específicamente para unir los puntos de vista de la empresa y TI, así como para crear el vínculo entre los activos de datos lógicos y físicos.

Ventaja: Contribución rápida y sencilla de todos los expertos en la materia para definir los procesos, las políticas y las entidades de datos de la organización para crear rápidamente una capacidad de gobierno de datos integral para los datos dentro del alcance.

3.3 Pregunta relativa a los puntos de entrada: ¿Cómo gestionamos los datos de los usuarios de datos?
Contexto: como resultado directo de la diversidad de uso de los datos en entornos de TI complejos, la creación de una visión única de toda la información de los usuarios de datos individuales resulta difícil. Este desafío deriva del hecho de que diferentes sistemas utilizan mecanismos muy diferentes para almacenar e indexar los datos. Sin una visión completa de los datos del usuario de datos individual y de cómo se almacenan, gestionan o procesan dentro de una organización, el cumplimiento del reglamento general de privacidad de datos será todo un desafío, especialmente en torno a los derechos de los usuarios de datos individuales.

Funcionalidades necesarias: La gestión de datos personales es una funcionalidad para identificar registros de usuarios de datos en todas las fuentes identificadas, cotejar y vincular registros entre sí para cada usuario de datos individual y crear un repositorio de Entity 360. Este repositorio ofrece una fuente de datos de gran calidad en la que se conservan registros de datos reales en las fuentes dentro del alcance y cómo cada fragmento de datos está vinculado a un objeto de datos individual. La Entidad 360 podría actuar como la fuente fidedigna de datos cuando las organizaciones responden a las solicitudes de acceso de los usuarios, al derecho de borrado o al derecho de solicitudes de portabilidad. Desde una perspectiva empresarial, la Entidad 360 puede ayudar a las organizaciones a gestionar el consentimiento para el uso de datos personales y, a continuación, gestionar este consentimiento: cuándo se ha otorgado/retirado, a través de qué canal y qué términos específicos se han acordado.

Caso de uso de tecnología: la gestión de datos personales puede caracterizarse como un caso de uso de correspondencia y vinculación de datos. Estas son las funcionalidades principales para identificar registros de usuarios de datos en los sistemas y proporcionar una vista transversal de los datos al cotejar registros entre sí y crear vínculos. Entre las funcionalidades típicas que se podrían aplicar a este caso de uso se encuentran:

- **Acceso a los datos relevantes:** Perfilar datos de usuarios de datos, extraer los datos relevantes de los sistemas de origen, aplicar procesos analíticos a contenido semiestructurado y no estructurado
- **Procesamiento de la calidad de datos:** evaluar los niveles de calidad de los datos, aplicar la corrección automática/manual, controlar los procesos para la corrección manual y elaborar informes de métricas
- **Fuente de datos única y fiable sobre los usuarios de datos, incluido el consentimiento, cómo se obtiene y cómo se gestiona:** incluye diferentes puntos de vista y perspectivas del usuario en función de sus consentimientos
- **Correspondencia y vinculación:** definir las reglas coincidentes basadas en definiciones de procesos de negocio, cotejar los registros, vincular los registros con la puntuación, asociar el consentimiento
- **Persistencia de datos:** mantener registros, análisis e informes vinculados/desvinculados

Soluciones tecnológicas: adoptar soluciones que ayudan a detectar registro de usuarios de datos de todos los dominios de datos, utilizando algoritmos avanzados para cotejar todos los datos relacionados con el mismo usuario de datos, independientemente de dónde se almacenan los datos. **Informatica Relate 360** utiliza algoritmos avanzados para identificar los datos asociados al mismo usuario de datos, la gestión de datos maestros proporciona la estructura para mantener y gestionar una vista común de los datos sobre los usuarios de datos.

Ventajas: una vista única de las personas ha demostrado tener beneficios empresariales más allá del reglamento general de privacidad de datos, sobre todo si la persona en cuestión es un cliente, que espera experiencias personales cada vez más adaptadas. Desde el punto de vista del reglamento general de privacidad de datos, la capacidad de vincular todos los datos de cada usuario de datos individual facilitará la tarea de habilitar los derechos de la persona. Esto incluye el derecho a comprender el uso de los datos, el derecho al olvido y la garantía de que el consentimiento se aplicará correctamente.

3.4 Pregunta relativa a los puntos de entrada: ¿Cómo puedo proteger los datos y evitar el acceso no autorizado?

Contexto: los controles de protección de datos son un enfoque para promulgar los requisitos del consentimiento del reglamento general de privacidad de datos y ayudar a proteger los datos personales. Puede haber un requisito de TI de eliminar, enmascarar o seudonomizar datos de producción utilizados para fines de prueba o de seudonomizar datos utilizados para transferencias de datos externos. El control de acceso a datos para los datos personales a nivel de usuario en las aplicaciones se debe revisar para fines de cumplimiento de normativas.

Funcionalidades necesarias: la **detección y protección** también proporciona controles de acceso y protección a la información sobre los usuarios de datos. La información de los usuarios de datos a menudo está expuesta a muchas personas de una organización y su ecosistema. Se utilizan controles de seguridad de los datos para eliminar u ocultar información sobre los usuarios de datos a quienes no deben poder verla y, al mismo tiempo, para poner la información a disposición de quienes deben verla.

Caso de uso de tecnología: la habilitación del control del consentimiento podría caracterizarse como un caso de uso de detección y protección. Estas son las funcionalidades principales para proteger y asegurar el acceso a los datos, aplicando controles centrados en los datos, como el enmascaramiento, el cifrado y el control de acceso, así como para gestionar el ciclo de vida de los datos, incluidos el archivado y la eliminación de datos y la aplicación. Entre las funcionalidades típicas que se podrían aplicar a este caso de uso se encuentran:

- **Aportación de los análisis de riesgos:** usar la puntuación de riesgo para dirigir los métodos de control de datos
- **Coordinación:** capacidad de programar y coordinar las tareas de protección de datos en función de los riesgos identificados y la supervisión del acceso o las condiciones inseguros
- **Controles de seguridad de datos:** enmascaramiento estático o dinámico, acceso seudonomizado y basado en funciones, cifrado o tokenización.
- **Historial de cambios/actualizaciones:** aplicación con respecto a los sistemas de origen, enmascaramiento de registros o archivado de resultados con respecto al registro de consentimiento, generación de pistas de auditoría para pruebas
- **Archivado:** archivar los datos de los sistemas de producción, registrar actividades para presentar pruebas, desconectarse para evitar el uso o acceso accidentales

Soluciones tecnológicas: adoptar soluciones que pueden ayudar a gestionar el ciclo de vida de los activos de datos y aplicar controles sobre estos activos. **Informatica Persistent Data Masking** e **Informatica Dynamic Data Masking** podrían utilizarse para ayudar a limitar de forma automática el número de personas y sistemas que tienen acceso ilimitado a los datos personales. **Informatica Secure@Source** proporciona la corrección de la seguridad de los datos al coordinar las actualizaciones de los controles de seguridad.

Ventajas: introducir la automatización en el enmascaramiento de datos para reducir el riesgo de filtraciones de los datos personales. La visibilidad de los datos personales está restringida a quienes tienen autorización para verlos, y los datos personales no proliferan sin la protección adecuada.

4. Socios

Como con muchas formas de reglamentación y cumplimiento, la tecnología por sí sola no garantiza el cumplimiento. Las organizaciones pueden necesitar el mejor liderazgo intelectual para su transición al reglamento general de privacidad de datos, así como la entrega de soluciones de tecnología y servicio tradicionales. Informatica trabaja junto con muchos socios cualificados y muy preparados para apoyarle en su iniciativa más amplia relacionada con el reglamento general de privacidad de datos. Estos socios se han elegido específicamente por sus profundos conocimientos de la gestión de datos, y su énfasis en el cumplimiento del reglamento general de privacidad de datos.

Encuentre al socio adecuado para usted, o póngase en contacto con su representante local de Informatica, que puede ayudarle a encontrar el mejor socio en función de sus necesidades y requisitos.

5. Conclusión

Este documento establece la necesidad de que las organizaciones reflexionen sobre las implicaciones del reglamento general de privacidad de datos. Este nuevo reglamento conlleva tanto desafíos como oportunidades para muchas organizaciones. Dado el corto periodo de tiempo hasta que este reglamento entre en vigor, muchas organizaciones deberán plantearse cómo afectará su interpretación de los principios del reglamento general de privacidad de datos a los procesos de gestión de datos actuales y futuros.

Para ayudar a las organizaciones a pasar rápidamente a la puesta en práctica de estas interpretaciones, Informatica ha descrito algunas de las preguntas relativa a los puntos de entrada fundamentales que los usuarios están formulando y ha sugerido algunas funcionalidades que serán necesarias para ayudar a responder a estas preguntas. Estas preguntas y funcionalidades no solo abordan una parte del conjunto de requisitos del reglamento general de privacidad de datos, sino que ayudan a desarrollar un conjunto de funcionalidades para abordar muchos de los desafíos que plantean los datos que conlleva el reglamento general de privacidad de datos.

En consonancia con cada funcionalidad, hay un caso de uso de tecnología. Cada caso de uso describe los tipos de soluciones de software y tecnologías que se podrían emplear para proporcionarlos.

Informatica ha sido el principal proveedor de gestión de datos durante más de 20 años y ha resuelto complejos desafíos de gestión de datos para miles de organizaciones de todo el mundo. El reglamento general de privacidad de datos creará muchos desafíos de gestión de datos complejos para muchas organizaciones. Informatica y su ecosistema de socios relacionados se encuentran en una posición ideal para ayudar a estas organizaciones con sus iniciativas relacionadas con el reglamento general de privacidad de datos.

6. Descargo de responsabilidad

El cumplimiento del reglamento general de protección de datos de la UE se basará en los datos específicos del negocio, las operaciones y el uso de los datos de una organización. Este documento proporciona un conjunto de puntos de debate que puede ser de utilidad en el desarrollo de los esfuerzos en materia de cumplimiento del reglamento general de privacidad de datos de la UE de una organización y no pretende servir como recomendaciones, directrices o asesoramiento legal. Todas las organizaciones deben consultar a su departamento legal interno acerca de las obligaciones que están o no están obligadas a cumplir.

Informatica

Informatica en España, José Echegaray 8, edif. 3, PB 3, 28232 Las Rozas, Madrid Teléfono: 902 882 062
www.informatica.com/es www.informatica.com linkedin.com/company/informatica twitter.com/Informatica

IN09_0218_03337