Impacto del RGPD en la gestión de acceso e identidad

Andrew Hindle (CIPP/E, CIPM, CIPT)

Tabla de contenidos

Resumen

Este artículo examina el alcance del Reglamento General de Protección de Datos ("RGPD", "Reglamento") en el diseño de sistemas y procesos de Gestión de Identidad y Acceso ("IAM"). Introduce buenas prácticas organizativas y técnicas que pueden ayudar a garantizar el cumplimiento demostrable del Reglamento, así como a mejorar la experiencia del usuario y la confianza del cliente.

Aunque el enfoque aquí está en el RGPD, los enfoques descritos pueden, por extensión, también ayudar a cumplir con la legislación de protección de datos en otras geografías, incluida, por ejemplo, la Ley de Privacidad del Consumidor de California ("CCPA") o la Ley General de Protección de Datos de Brasil (“LGPD”).

Unas palabras al lector

Para la comprensión de este artículo asumimos al menos un conocimiento básico de los temas relacionados con la protección de datos y privacidad, en particular, de RGPD y de los principios básicos descritos en las pautas de privacidad de la OCDE. Incluso si no es un oficial de seguridad o privacidad en su organización, comprender las reglas lo ayudará a tener mejores conversaciones con sus pares acerca de la privacidad.

El panorama de la regulación de la privacidad está evolucionando rápidamente. Por lo tanto, el asesoramiento brindado aquí no puede ser exhaustivo y no pretende ni debe considerarse como un sustituto del asesoramiento legal. Si bien es importante para el profesional de la identidad digital un buen conocimiento y comprensión de las consideraciones de privacidad, no podemos esperar que la mayoría de los profesionales sean abogados especializados en privacidad. Al igual que con cualquier área de regulación, si no está seguro, siempre es mejor buscar asesoramiento profesional.

A lo largo del artículo, se subrayarán consejos específicos de "buenas prácticas técnicas"; estos consejos también se recopilan en una sección al final del artículo como una lista de verificación a seguir para las buenas prácticas de IAM.

Introducción

Las convenciones, regulaciones y leyes de privacidad existen desde hace mucho más tiempo de lo que la mayoría de la gente cree. Ya en 1948, la Asamblea General de las Naciones Unidas consagró el derecho a la privacidad en el artículo 12 de la Declaración Universal de los Derechos Humanos. En 1980, la OCDE emitió sus “Directrices sobre la

protección de la privacidad y los flujos transfronterizos de datos personales", que fueron revisadas y actualizadas significativamente en 2013 (q.v.).

Los países individuales y los bloques comerciales más amplios continúan desarrollando sus regulaciones de privacidad y protección de datos, en parte para dar cuenta de la evolución de la tecnología. No es raro que los marcos regulatorios vayan a la zaga de los desarrollos tecnológicos, pero se seguirán realizando cambios a la luz del impacto que trae Internet, los dispositivos conectados, la inteligencia artificial y la genómica. Para agregar complejidad, la mayor movilidad global de las personas sugiere que los cambios locales en la protección de datos y la regulación de la privacidad impactan en los cambios en otras jurisdicciones. Además de los cambios en Europa, en los últimos años han surgido regulaciones de privacidad actualizadas en Brasil, Singapur, Filipinas, China y algunos lugares de los Estados Unidos, por nombrar algunos.

Esta evolución de la regulación es importante. Cuando se ve a través de la lente de un panorama regulatorio en constante cambio y evolución, podemos ver el RGPD (y otras regulaciones de privacidad modernas) como un conjunto de herramientas que pueden ayudarnos a construir mejores sistemas, no solo como un conjunto de casillas de verificación que necesitamos marcar.

Incluso si trabaja para una organización que no hace negocios directamente con Europa, varios elementos del RGPD tienen un impacto global. Otras regulaciones de privacidad puedan contener disposiciones similares; aunque no sería prudente planificar la armonización global de estas regulaciones, cada vez hay más puntos en común entre las geografías. También debemos reconocer que el RGPD se aplica por igual a cualquier información sobre personas, ya sean datos dentro de una empresa sobre sus empleados o datos sobre personas externas como clientes. En otras palabras: el RGPD realmente nos impacta a todos.

El Reglamento incluye un requisito de protección de datos por diseño. Dejando de lado la necesidad específica de cumplir con el Reglamento, estos son fundamentalmente buenos principios de diseño. Ayudan a mitigar el riesgo comercial (por ejemplo, cuantos menos datos tenga, menor será el interés de atacarlo y menor será el impacto de cualquier ataque) y ayudan a reducir los gastos administrativos generales y el esfuerzo desperdiciado (por ejemplo, cuantos menos datos tenga, menos probable es que tenga registros duplicados o contradictorios).

Por definición, dado que el RGPD se ocupa de los datos personales, estos principios tienen implicaciones significativas sobre cómo diseñamos e implementamos sistemas que utilizan dichos datos, incluidos los sistemas y procesos de IAM. De hecho, sin una base IAM que cumpla con el Reglamento, simplemente no es posible que un producto final cumpla con el mismo. (No obstante, tome en cuenta que aunque los propios sistemas y procesos de IAM

estén listos para la regulación, ¡aún debe asegurarse de que el servicio final también cumpla con la misma!).

El resto de este artículo explorará las principales consideraciones que deben tener los equipos al desarrollar proyectos de IAM que puedan cumplir con las necesidades del Reglamento.

El Reglamento se aplica tanto a la representación física de datos (como en papel) como a los datos digitales. Nos centraremos aquí en la información digital, pero haremos referencia cuando corresponda a algunas implicaciones específicas (por ejemplo, en las áreas de depuración, informes de gestión, etc.)

Comenzaremos con algunas observaciones generales, incluidos comentarios sobre la composición y la estructura del proyecto de su equipo de proyecto. Luego nos centraremos en las cuatro etapas por las que pasan los datos, incluidos los datos personales, durante su ciclo de vida: crear, leer, actualizar y eliminar. Para cada una de estas etapas, haremos referencia a algunas de las áreas específicas del RGPD que se aplican e identificaremos algunas arquitecturas, herramientas y técnicas que pueden ayudar. Cuando sea relevante, notaremos las diferencias que podrían aplicarse si usted es un 'controlador de datos' o un 'procesador de datos', pero en su mayor parte, es más probable que el impacto de estas diferencias sea a nivel comercial/legal, y no a nivel técnico. Terminaremos con un resumen de los puntos clave que también se pueden usar como un recordatorio rápido para proyectos futuros o la capacitación del equipo.

Terminología

- Mapeo de datos: "un sistema de **catalogación de los datos que recopila**, cómo se usan, dónde se almacenan y cómo viajan a través de su organización y más allá de ella".[1]
- Oficial de protección de datos (DPO, por su sigla en inglés): una persona que debe ser designada en cualquier organización para procesar datos definidos por el RGPD como confidenciales.[2] El DPO es responsable de “Trabajar para el cumplimiento de todas las leyes de protección de datos relevantes, monitorear procesos específicos, como las evaluaciones de impacto de la protección de datos, sensibilizar a los empleados en el área de protección de datos y capacitarlos en consecuencia, así como colaborar con las autoridades supervisoras.” (Consulte los artículos 35, 37, 38 y 39 del RGPD para obtener más detalles)
- Datos personales - Los datos personales son cualquier información relacionada con una persona física identificada o identificable.[3] (Consulte el artículo 4 (1) del RGPD para obtener más detalles).

- Protección de datos por diseño: protección de datos a través de la tecnología adecuada y medidas organizativas.[4] Consulte el artículo 25 del RGPD para obtener más detalles.

Observaciones generales

Colaboración con asesores de privacidad

Teniendo en cuenta los principios de Protección de datos desde el diseño y por defecto, tal como se define en el artículo 25 del RGPD, quizás la acción más crítica que se puede tomar es asegurarse de que los requisitos de privacidad se consideren desde el comienzo de cualquier proyecto.

El RGPD requiere que muchas organizaciones (pero no todas) tengan un Oficial de Protección de Datos ("DPO") designado. Las organizaciones más grandes pueden tener un equipo de asesores de privacidad. Si está liderando un proyecto que involucra datos sobre individuos, es su responsabilidad asegurarse de que sus colegas de privacidad estén involucrados. Asegúrese de involucrar a las personas relevantes en su proyecto desde la etapa más temprana. ¡Recuerde que es posible que no conozcan su proyecto a menos que usted se lo diga! No tema preguntar quién está involucrado desde el punto de vista de la privacidad y luego desarrolle una relación de trabajo con su asesor.

Es posible que su especialista en privacidad (si no tiene un DPO experimentado) no tenga una formación técnica profunda, por lo que deberá asegurarse de proporcionarle la información que necesita en un formato que tenga sentido para él para que pueda brindar un asesoramiento completo e integral. Para que las conversaciones sean más productivas y eficientes, considere realizar lecturas adicionales sobre privacidad o incluso investigar calificaciones o certificaciones reconocidas públicamente de organismos comerciales de privacidad relevantes u otras instituciones como parte de su desarrollo profesional continuo.

Planteamiento de inquietudes/denuncia de irregularidades

Si le preocupa que su proyecto o su organización no se esté tomando la privacidad lo suficientemente en serio, o si cree que ha identificado un problema que lo deja fuera del cumplimiento del RGPD o, en el peor de los casos, una violación de datos real, asegúrese de conocer los canales correctos a través de los cuales pueda informar sobre esto. Las organizaciones más grandes deben tener mecanismos bien establecidos para escalar un problema y denunciar una situación, y también es probable que tengan políticas y procesos de denuncia de irregularidades que puede utilizar como último recurso. Es posible que las organizaciones más pequeñas no lo hagan, por lo que deberá usar su mejor criterio profesional para determinar cómo plantear las inquietudes de manera más

efectiva. Mantenga buenos registros de tales conversaciones, pero **no** incluya ejemplos específicos de datos personales cuando informe problemas si se pueden evitar, esto con el fin de que no empeore una violación de datos (o, sin darse cuenta, convierta un incidente potencial en una violación de datos real).

Finalmente, si su organización tiene un DPO[5], recuerde que el RGPD impone requisitos bastante estrictos sobre la relación independiente y las líneas de información del DPO. Estas pueden ser garantías útiles si descubre que necesita escalar la situación.

Datos personales – definición y mapeo

El RGPD tiene una definición muy amplia de lo que se considera datos personales: "'datos personales' significa cualquier información relacionada con una persona física identificada o identificable ('sujeto de datos'); una persona física identificable es aquella que puede identificarse, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos del estado físico, fisiológico, identidad genética, psíquica, económica, cultural o social de esa persona natural".[5]

Es importante, entonces, ser igualmente amplio en su enfoque. Considerando todo el proyecto, asegúrese de comprender íntegramente cuándo los datos podrían pertenecer a la categoría de datos personales. Recuerde que incluso si está tratando con datos agregados o seudónimos, el Reglamento seguirá aplicándose si esos datos pueden ser "re-identificados".

Al comienzo de un proyecto, considere un proceso conocido como "mapeo de datos" para descubrir y mapear qué datos personales podrían usarse, dónde y cómo, y monitorear y actualizar este mapa de datos durante todo el ciclo de vida del proyecto. El mapeo de datos es "un **sistema de catalogación de los datos que recopila**, cómo se usan, dónde se almacenan y cómo viajan a través de su organización y más allá de ella". Dicho proceso suele ser parte de una evaluación de impacto de protección de datos (DPIA, por su sigla en inglés), pero también puede ser útil en el diseño general de su arquitectura IAM, por lo que nunca es un esfuerzo en vano.

Tecnologías de seguimiento individual

El uso de tecnologías de seguimiento individuales, incluidas, entre otras, las *cookies*, requiere (al momento de redactar este documento) más que solo el RGPD para considerar si un servicio o sitio web incluye su uso. Cada Estado miembro de la UE es responsable de emitir su propia guía de acuerdo con esta directiva, lo que ha dado lugar a algunas divergencias importantes en esta área; la jurisprudencia sigue evolucionando.

Sin embargo, algunas *cookies* pueden estar sujetas al RGPD si, por ejemplo, contienen información que podría usarse (quizás junto con otros datos) para identificar a una persona. Por lo tanto, aunque tal vez no sea una consideración central para el profesional de IAM, vale la pena estar al tanto y estar alerta a los posibles problemas en esta área.

Circunstancias especiales

La orientación proporcionada en este artículo pretende ser de aplicación general a todos los proyectos de IAM. Sin embargo, algunos proyectos tendrán circunstancias particulares que ameritan atención y consideración adicionales. Algunas de estas circunstancias incluyen niños, aplicación de la ley y ciertos datos de categorías especiales. En todos los casos, los profesionales deben buscar orientación legal independiente.

Categoría especial y otros datos confidenciales

El RGPD establece disposiciones especiales para ciertos tipos de datos más sensibles, que incluyen (pero no se limitan a) raza, orientación sexual, afiliación política y religiosa, datos relacionados con la salud y datos biométricos.[6] Si está manejando datos de categoría especial en estas áreas, necesitará medidas de seguridad adicionales.

Infantes

Si su proyecto involucra datos sobre niños, también deberá tener especial cuidado. El RGPD define a un niño como una persona menor de 16 años, pero tenga en cuenta que cada país puede (y algunos, incluido el Reino Unido, lo han hecho) reducir este límite a la edad de 13 años o menos.[6]

Cumplimiento de la ley y datos personales

El uso de datos personales por parte de los organismos encargados de hacer cumplir la ley está sujeto a directivas, reglamentos y leyes independientes; éstos no se consideran en este artículo.

Procesamiento automatizado, aprendizaje automático e inteligencia artificial

El tratamiento automatizado de datos personales es una circunstancia especial por derecho propio, pero que merece una atención particular. El procesamiento automatizado puede incluir todo, desde el aprendizaje automático (ML, por su sigla en inglés), el procesamiento algorítmico, el uso de tecnologías de cadena de bloques o la inteligencia artificial (AI, por su sigla en inglés). AI/ML, en particular, es un campo de rápido

movimiento; desarrolladores, especialistas en ética, legisladores y reguladores en todo el mundo aún intentan medir el alcance completo de lo que podría ser posible. Ya está claro que los sistemas AI/ML pueden inferir o deducir "hechos" sobre personas que no formaban parte del conjunto de datos original (a menudo vemos esto en la elaboración de perfiles de usuarios). También está claro que un conjunto de datos original puede no contener datos personales (por definición), pero sí contenerlos una vez procesado.

Está más allá del alcance de este artículo explorar esta área en profundidad; Sin embargo, el RGPD impone requisitos bastante estrictos en el caso de la toma de decisiones y elaboración de perfiles automatizados.[1]

Greenfield/Brownfield[2]

El RGPD en sí mismo no hace distinción entre las aplicaciones totalmente nuevas (*Greenfield*) y la refactorización de las aplicaciones existentes (*Brownfield*) para llevarlas a cumplir con la norma. Desde un punto de vista práctico, el primer caso ofrece un camino más fácil para usar técnicas y estándares modernos y, muy seguido, está menos entorpecido por los requisitos heredados de integración/soporte.

Sin embargo, tenga en cuenta que el cumplimiento del RGPD puede llevarlo a revisar todas las aplicaciones en el entorno de trabajo de su proyecto. En algunos casos, habrá (más o menos) soluciones técnicas o de procedimiento simples para lograr el cumplimiento. En otros, sin embargo, es posible que deba revisar los objetivos comerciales originales a la luz del Reglamento.

Proxy/Acceso delegado

Este artículo parte de la suposición general de que un sujeto de datos proporcionará y/o accederá a datos sobre sí mismo. Dicho esto, naturalmente hay una variedad de casos en los que alguien podría acceder legítimamente a los datos en nombre de un tercero.

En tales circunstancias, es crucial establecer y aplicar mecanismos apropiados de autenticación, identificación y autorización (como se recomienda de diversas formas, más adelante en este artículo) tanto para el titular de los datos originales como para su apoderado, junto con el consentimiento de delegación. En algunas circunstancias, el consentimiento puede surgir a través de instrumentos legales como un poder notarial, una orden judicial o similar. Establezca si este es un requisito para su caso de uso y diseñe los

[1] Vea el artículo 22 de la regulación.

[2] *Greenfield* es un término utilizado para describir un proyecto sin trabajo previo que limite su desarrollo. *Brownfield*, por el contrario, se refiere a proyectos con limitaciones predeterminadas basadas en tener que trabajar en una plataforma existente o bajo restricciones preexistentes.

procesos en consecuencia. También debe considerar seriamente mantener un registro de consentimiento de delegación y otras acciones de autorización cuando corresponda. Estándares como UMA y un recibo de consentimiento pueden ayudar en este sentido.

Copias de seguridad

Tener un mecanismo confiable para asegurar sus datos en caso de un desastre no solo es una buena práctica general, también es, esencialmente, un requisito del RGPD. Recuerde, sin embargo, que un mecanismo de copia de seguridad mal diseñado puede ponerlo en mayor riesgo de sufrir una infracción. Asegúrese de que los datos de cualquier copia de seguridad estén protegidos con un cifrado fuerte y con otras herramientas que incluyen, entre otras, acceso privilegiado/administración de usuarios, aunque tenga en cuenta que estas protecciones pueden complicar el proceso de restauración. Ciertos sectores o aplicaciones también pueden requerir un mecanismo de respaldo físico o en papel. Si bien es probable que esto quede fuera del alcance inmediato de la responsabilidad del profesional de la identidad digital, tenga en cuenta que los requisitos del RGPD se aplican por igual a los datos en formato físico. Las copias de seguridad también introducen una complejidad adicional en el área de la retención.

El trayecto de los datos

Paso uno - Crear

La primera etapa del trayecto de nuestros datos, "crear", comienza en el momento en que se propone recopilar datos personales. No confunda esto con el momento en que escribe los datos en una base de datos (u otro mecanismo de almacenamiento). Antes incluso de solicitar datos de (o sobre) el sujeto de datos, debe comprender claramente y comunicarle lo que está recopilando y por qué, además de describir sus derechos como sujeto de datos. Estos se expresan más comúnmente a través de un aviso de privacidad que utiliza un lenguaje claro y sencillo, ¡y al menos debe asegurarse de que el aviso refleje con precisión la forma en que su sistema realmente funciona!

Dependiendo de la base legal para procesar los datos relevantes, es posible que deba obtener el consentimiento del interesado para recopilar y procesar su información. La forma en que obtenga el consentimiento diferirá de un proyecto a otro, según los datos que se recopilen y para qué se utilicen. Su asesor de privacidad puede brindarle orientación.

Desde una perspectiva de auditoría, considere mantener un registro de ese consentimiento y/o proporcionarle a su sujeto de datos un registro para ellos mismos; aquí pueden aplicarse estándares en evolución, como el recibo de consentimiento. ¡Recuerde, sin embargo, que cualquier recibo o registro puede contener datos personales!

Crear mínimamente

Si la protección de datos por diseño y por defecto constituyó el primer principio rector de su proyecto, entonces su segundo principio rector debería ser el de minimizar los datos recopilados. Minimizar los datos es una buena práctica, independientemente de los requisitos de cumplimiento: cuanto menos recopile o procese, menos tendrá que proteger y administrar con el tiempo. También es uno de los 7 principios que establece el RGPD para el tratamiento de datos personales.

El resultado final: al recopilar datos de un sujeto, recopile y conserve l**a menor cantidad de datos posible** para cumplir con sus requisitos. Del mismo modo, para los datos indirectos sobre un sujeto de datos, como las huellas dactilares del navegador, recopile y conserve la menor cantidad de datos posible. Esto significa que debe tener una buena comprensión de la lógica comercial del proyecto, de modo que tenga clara la justificación y pueda ayudar a sus colegas en el lado comercial a cumplir con sus obligaciones: siempre es útil preguntar *por qué* una pieza determinada de información debe ser recopilada.

Recuerde que el RGPD considera los datos en conjunto. Considere si existe alguna posibilidad de que los datos que recopila su proyecto se combinen con otros datos que posee la organización de tal manera que puedan resultar en la identificación del individuo (consulte también "leer" a continuación). Evite la recopilación repetida de datos que su organización ya tiene sobre un individuo. Además de ser una experiencia frustrante para el usuario, esto también da como resultado registros duplicados o contradictorios, lo que puede causar problemas con la precisión de los datos, las solicitudes de acceso de los sujetos, la eliminación y otras áreas del Reglamento. Si tiene un mapa de datos grande y dispar, considere usar herramientas de descubrimiento de datos o de metadirectorio para ayudar con la visibilidad y la consolidación.

Tenga en cuenta que puede estar recopilando datos *implícitos* o inferidos, que también pueden calificar como datos personales: direcciones IP, por ejemplo, o análisis del sistema. Estos deberán manejarse con la misma diligencia que los datos que solicita *explícitamente* de un interesado o en su nombre. Incluso si estos datos se recopilan y utilizan de manera transitoria, aún deben manejarse correctamente.

Considere también formas creativas de limitar la cantidad de datos que recopila. Además de simplemente recopilar menos, una organización podría utilizar un servicio de atributos para responder a preguntas como "¿el sujeto de los datos tiene más de 18 años?", en lugar de recopilar y almacenar la fecha de nacimiento del sujeto, o exigirles que divulguen la información de la tarjeta de crédito. También vale la pena investigar las tecnologías que pueden proporcionar evidencia de que una autoridad tiene conocimiento de cierta información sin revelar la información en sí misma (prueba de conocimiento cero[8], por ejemplo). Tenga en cuenta, sin embargo, que es posible que los requisitos legales existentes aún no tengan en cuenta dichas tecnologías.

Como se señaló anteriormente, este artículo considera principalmente el impacto del RGPD en la identidad digital. Sin embargo, el momento de la recopilación/creación de datos es a menudo donde ocurren los procesos en papel. Incluso si estos no son su preocupación directa, no es una mala práctica asegurarse de comprender cómo se procesan los registros en papel.

Posibilidades de federación

Habiendo tratado con los conceptos básicos, ahora debe hacer una pregunta importante: ¿su caso de uso realmente necesita la creación de una cuenta de usuario completa? Hay una tendencia, nacida de años de experiencia, a gravitar hacia esto como el primer puerto de escala en cualquier proyecto de identidad. Sin embargo, en muchos casos, es innecesario; o es algo que solo se necesita más adelante. Los estándares establecidos como SAML u OpenID Connect admiten la federación de identidad transitoria; esto es a menudo todo lo que necesita. En tal caso, solo está manejando datos personales (si es que lo hace) durante un breve período de tiempo, por lo que los principios normales de minimizar los datos recopilados y las precauciones para los datos en tránsito pueden ser suficientes. (utilice la versión más reciente de TLS, además de cifrado de datos específico adicional según sea necesario)

Si necesita una cuenta de usuario por razones técnicas (persistencia de datos de sesión, por ejemplo), ¿podrá hacerse esencialmente "impersonal" mediante el uso de (por ejemplo) una federación seudónima? Usar seudónimos permite comparar la identidad del usuario mediante un identificador que no se puede asociar fácilmente con una persona conocida. Sin embargo, tenga cuidado en este caso: puede ser posible combinar datos de tal manera que se vuelva a identificar la información, anulando así el propósito de usar seudónimos. Los datos seudónimos aún se consideran datos personales y, como tales, deben considerarse de acuerdo con los requisitos del RGPD.

Almacenamiento de datos

Si considera que necesita conservar los datos, ya sea con seudónimo o no, deberá pensar dónde y cómo almacena los datos. Las protecciones habituales para los datos en reposo son importantes. Utilice técnicas de encriptación apropiadas y manténgalas bajo revisión de rutina: la criptografía es un área de rápido desarrollo (particularmente dado el advenimiento de la criptografía cuántica y la evolución de los algoritmos y técnicas "seguros cuánticamente"). También debe asegurarse de que se implementen los procesos correctos para mantener los sistemas, las aplicaciones y las bibliotecas de soporte actualizados y con parches.

A pesar de otros requisitos de RGPD, los patrones de diseño de aplicaciones modernas casi seguramente lo llevarán a proporcionar una API para manejar sus datos personales. En tales casos, el acceso a dichas API debe estar protegido, idealmente utilizando un protocolo

como OAuth; también podría considerar usar una puerta de enlace API. Volveremos a la protección de API más adelante en nuestro trayecto de los datos.

Si está considerando una solución de almacenamiento utilizando un libro mayor distribuido, debe tener mucho cuidado. Ahora existe un claro consenso de que almacenar datos personales directamente en dicho libro no es una buena práctica. Algunas soluciones que se están desarrollando actualmente pueden evitar este escollo en particular, pero aun así vale la pena tenerlo en cuenta, especialmente si está creando la suya propia. Hasta que esta área de la tecnología sea más estable, el mejor consejo es proceder con cautela; mantener dichos proyectos bajo revisión periódica regular, incluso después del despliegue; y para asegurarse de que tiene una forma bien documentada y de fácil implementación para revertir el uso de la solución basada en el libro mayor, en caso de que sea necesario.

El uso de un almacén de datos o de usuarios basado en la nube puede tener beneficios desde una perspectiva de gestión de riesgos y privacidad. Asegúrese de trabajar con su equipo de privacidad para que su aviso de privacidad refleje con precisión la relación entre usted y su proveedor.

Ubicación del almacenamiento de datos

El RGPD en sí mismo no impone requisitos de territorialidad de los datos, es decir, no requiere que los datos se almacenen en una geografía particular, aunque las regulaciones en otras jurisdicciones sí lo hacen. Debe, como mínimo, desarrollar una arquitectura flexible que le permita separar los datos por región en caso de que sea necesario, aunque tenga en cuenta que esto podría significar recopilar datos personales adicionales que, de otro modo, no necesitaría.

Dicho esto, el RGPD **tiene** requisitos en torno a la transferencia de datos fuera de la Unión Europea (es decir, a un "tercer país"). La transferencia de datos personales a cualquier tercer país siempre debe ser una preocupación importante en el contexto de RGPD y, aunque ciertamente se pueden idear soluciones, esta es un área de desarrollo regulatorio continuo. Necesitará una discusión cuidadosa con su asesor de privacidad para asegurarse de que esto se esté manejando correctamente.

Paso 2 – Leer

Todos y cada uno de los accesos a los datos personales que posee deben mantenerse seguros. En el nivel más básico, esto significa asegurarse de minimizar dicho acceso. Si aún no lo está haciendo, considere implementar una solución de administración de usuarios/acceso privilegiado cuando corresponda. También debe asegurarse de que incluso aquellos usuarios privilegiados autorizados, incluidos los administradores de sistemas y bases de datos, no puedan acceder a los datos personales en forma clara, ni siquiera accidentalmente. Recuerde que **cualquier** acceso no autorizado a los datos

personales constituye una posible violación de datos. Tal incumplimiento puede ser más o menos grave y tener mayores o menores consecuencias... pero sigue siendo un incumplimiento.

Para proporcionar una funcionalidad útil y evitar una posible violación de datos, asegúrese de utilizar métodos modernos y seguros para autenticar y autorizar a sus usuarios, tanto internos como externos. Utilice múltiples factores de autenticación; considere los autenticadores FIDO; evite SMS como un factor; Considere los estándares de autorización modernos (y los productos que los respaldan), incluidos protocolos establecidos como XACML, estándares más nuevos como el acceso administrado por el usuario ("UMA") y enfoques emergentes como la autorización transaccional.

Tenga en cuenta que "autenticación" no es necesariamente lo mismo que "verificación". Es posible que no necesite establecer la identidad física real del usuario en ningún nivel de seguridad para satisfacer su solicitud de manera segura. Sin embargo, cuando se requiera cierto nivel de garantía de una identidad del mundo real, recuerde tratar los datos utilizados para verificar la identidad del usuario con un nivel de seguridad adecuado.

Si está completando previamente formularios visibles para el cliente, tenga especial cuidado de que dichos datos solo se muestren al usuario debidamente autorizado y que no se puedan almacenar en caché a través de las visitas de diferentes usuarios.

Los patrones de diseño de aplicaciones modernas probablemente significarán que tiene una API para operaciones de "lectura". Como se señaló anteriormente, cualquier API de este tipo debe estar debidamente protegida. Considere también agregar protecciones adicionales a nivel de programa o sistema: por ejemplo, protección contra lecturas secuenciales múltiples al requerir autorización adicional o al imponer un límite de lectura total o una restricción de tiempo de repetición.

Sea consciente de otros sistemas que pueden tener acceso a datos personales: aplicaciones de seguridad (especialmente soluciones basadas en ML o IA) y herramientas de minería de datos, por ejemplo. Asegúrese de que dichos sistemas no tengan acceso no autorizado o innecesario a los datos personales y tenga en cuenta que, en algunos casos, dicho acceso podría constituir una toma de decisiones o elaboración de perfiles automatizada (como se mencionó anteriormente).

Considere también las consecuencias no deseadas. Si tiene una herramienta de informes que (por ejemplo) genera una hoja de cálculo de datos de Excel que luego se puede enviar por correo electrónico, considere (a) sí toda la información personal de identificación debe estar allí; y (b) si puede proporcionar protección de forma automática por adelantado (por ejemplo, mediante la creación automática de una hoja cifrada, en lugar de confiar en que el usuario lo haga por sí mismo), para ayudar a reducir aún más el riesgo de una infracción accidental más adelante.

Solicitud de acceso a datos personales y portabilidad de los datos

El sujeto de los datos personales tiene derecho, en virtud del RGPD, a acceder a los datos personales que usted tiene sobre ellos[8.] Esto presenta un riesgo de incumplimiento evidente. Si está manejando una respuesta a una solicitud de acceso de un sujeto de datos, o si está diseñando un sistema para tal caso, entonces debe tener especial cuidado para asegurarse de autenticar y/o verificar correctamente al usuario; que estén debidamente autorizados; y que los datos que comparte no contienen datos personales de otros interesados.

El RGPD también le exige que proporcione todos los datos personales del sujeto en un formato legible por máquina para la portabilidad de los datos. Las mismas consideraciones de seguridad se aplican en este caso.

De manera un tanto perversa, para ayudar a satisfacer algunos de estos requisitos, es posible que deba recopilar (o inferir) más datos personales de los que preferiría, aunque siempre debe tener cuidado de no recopilar más datos de los que realmente necesita. Por ejemplo: es posible que deba establecer en qué país vive, está o es ciudadano un usuario determinado, para establecer qué legislación se aplica. Según el diseño de su sistema, tal vez pueda evitar almacenar esta información y, en su lugar, solicitarla en tiempo real cuando sea necesario tomar una decisión (y verificarla según sea necesario).

Informe de violación de datos

El informe de violación es un caso especial en el contexto de "lectura": si debe informar una infracción o una posible infracción, debe asegurarse de no enviar datos personales como parte de su informe. Si tiene herramientas automatizadas de informes de violación o de seguridad, asegúrese de que estas herramientas no creen o empeoren accidentalmente una infracción al incluir datos personales en sus informes. Considere también el uso de soluciones de software de privacidad que pueden ayudar a buscar en conjuntos de datos de forma segura.

Paso 3 - Actualización

El RGPD exige que el interesado pueda corregir fácilmente cualquier dato personal que tenga sobre él. Asegúrese de que su sistema cuente con dicho mecanismo. Las soluciones de autoservicio para el usuario pueden ser especialmente útiles en este sentido, siempre que sean fáciles de encontrar y utilizar. Una vez más, la autenticación adecuada y, en algunos casos la verificación, son cruciales para mitigar una posible infracción accidental.

Vale la pena señalar que este requisito de "actualización" del Reglamento puede tener implicaciones para las soluciones basadas en registros distribuidos. En particular, debe

establecer si dicha solución permitirá la rectificación de un registro histórico en el libro mayor (o en la cadena). Es poco probable que sea suficiente simplemente marcar el registro histórico como "ya no está activo".

Paso 4 - Borrar

En algunos casos, el RGPD otorga al interesado el derecho a solicitar que se eliminen los datos que tiene sobre él. Deberá asegurarse de tener una forma sencilla de hacerlo, y que este mecanismo esté protegido contra el uso indebido accidental o deliberado con las medidas de seguridad adecuadas, incluidos los niveles y métodos necesarios de autenticación y autorización. Considere mantener registros de auditoría para tales transacciones (teniendo en cuenta que querrá mantener los datos personales reales fuera del registro) y, potencialmente, tener un mecanismo de "retroceso" de tiempo limitado en caso de error.

El Reglamento también requiere que los datos se almacenen solo durante el período en que realmente se necesitan. Los requisitos comerciales, informados por las necesidades de privacidad, dictarán la duración del período de retención; pero deberá diseñar su sistema de manera que los datos puedan eliminarse fácilmente al final de este período. Considere mantener un registro separado que indique cuándo se crearon originalmente los datos en cuestión y ejecutar una tarea automatizada para informar sobre los datos que han llegado a su fecha de retención (por lo tanto, marcarlos para su eliminación manual) o para eliminarlos directamente.

Para implementaciones grandes y/o *brownfield*, es posible que deba ejecutar un proceso de descubrimiento para establecer qué datos tiene realmente sobre un sujeto de datos determinado. Existe una variedad de soluciones de software que pueden facilitar esta tarea.

Al igual que con 'Actualizar', si tiene una API (u otra instalación) que puede realizar la eliminación de datos, y especialmente si permite la eliminación masiva, asegúrese de protegerse contra el uso indebido. Por ejemplo: agregue una verificación adicional antes de una eliminación masiva (incluso manual) o solicite una autorización adicional para las solicitudes que excedan un cierto número de registros. También debe asegurarse de tener una forma de hacer una copia de seguridad de los datos de forma rutinaria y restaurarlos en caso de error (o un intento deliberado de corromper los datos), y considere forzar una copia de seguridad a través de su código API antes de que se ejecute el proceso de eliminación. Recuerde que la conservación de dichas copias de seguridad debe ser limitada.

Conclusión

El RGPD, y otras leyes y regulaciones modernas de protección de datos y privacidad, nos llevan a tener especial cuidado en el diseño, desarrollo y mantenimiento de nuestras soluciones IAM. En particular:

- Recopilar solo los datos que necesitamos
- Guardarlos solo el tiempo que sea necesario
- Protegerlos cuando esté a nuestro cuidado
- Asegurarse de que solo puedan acceder aquellos que deberían tener acceso
- Asegurarse de que se puedan actualizar adecuadamente
- Desecharlos de forma segura cuando sea el momento de hacerlo.

Ya tenemos las herramientas que necesitamos para hacer esto, pero debemos tener cuidado de aplicar esas herramientas de la manera correcta y asegurarnos de que los dueños de negocios no nos pidan que hagamos cosas que no deberíamos estar haciendo:

- Solo cree cuentas si es absolutamente necesario; use federación (SAML; OpenID Connect) u otra información transitoria o no identificable donde se pueda (Información de usuario; Pruebas de conocimiento cero)
- Autentique a los usuarios, preferiblemente con factores de autenticación fuertes y múltiples (FIDO)
- Autorice usuarios, preferiblemente con protocolos modernos (XACML y UMA)
- Proteja las API (OAuth)

Mucho de lo que necesitamos hacer no es nuevo, y en su mayoría es considerado como una buena práctica. Simplemente no ha sido necesariamente una práctica estándar o incluso, una de las primeras consideraciones en la lista para los proyectos. Las nuevas regulaciones de privacidad nos dan la oportunidad de hacer las cosas de la manera correcta.

Lista de verificación de su proyecto IAM

- Asegúrese de que los requisitos de privacidad se consideren desde el comienzo de un proyecto y se vuelvan a evaluar de forma rutinaria durante la vida útil de la aplicación.
- Desde la etapa más temprana de su proyecto, involucre a las personas relevantes (personas que representan a las organizaciones que consumen los datos de IAM, así como aquellos que sirven como fuentes de verdad para sus datos de IAM, junto con sus pares de privacidad).
- Mantenga buenos registros de cualquier conversación sobre posibles violaciones de datos, pero no incluya ejemplos específicos de datos personales cuando reporte problemas.
- Mapee qué, dónde y cómo se pueden usar los datos personales; este será un aporte valioso para una Evaluación de Impacto de Protección de Datos (DPIA, por sus siglas en inglés) más completa.
- Si está manejando datos de categoría especial según lo definido por RGPD y/o sus regulaciones de privacidad locales o sectoriales, necesitará medidas de seguridad adicionales.
- Si su proyecto involucra datos sobre niños, también deberá tener especial cuidado.
- ¡Asegúrese de que el aviso de privacidad de su organización o servicio refleje con precisión la forma en que realmente funciona el sistema!
- Recabe el consentimiento del interesado para que recopile y procese su información.
- Mantenga un registro de ese consentimiento y/o proporcione a su sujeto de datos un registro para ellos mismos.
- Explore la especificación de recepción de consentimiento y las implementaciones emergentes.
- Recopile la menor cantidad de datos posible (minimice la recopilación de datos).
- Evite la recopilación repetida de datos.
- Considere el uso de herramientas de descubrimiento de datos o metadirectorio para ayudar con la visibilidad y la consolidación.
- Explore tecnologías e implementaciones a prueba de conocimiento cero e investigue si dichas soluciones debieran formar parte de su implementación.
- En lugar de crear una cuenta, considere usar la federación de identidad transitoria y/o el inicio de sesión único. Si no se puede evitar la creación de una cuenta, considere usar la federación seudónima y/o el inicio de sesión único para reducir la cantidad de datos personales identificables que posee.
- Use la versión más reciente de TLS más el cifrado de datos específico adicional según sea necesario.
- Utilice técnicas de encriptación apropiadas y manténgalas bajo revisión de rutina.
- Mantenga los sistemas, las aplicaciones y las bibliotecas de soporte actualizados y con parches.

- Proteja el acceso a las API que manejan datos personales, idealmente utilizando un protocolo como OAuth.
- El almacenamiento de datos personales directamente en un libro mayor distribuido no es una buena práctica.
- Desarrolle una arquitectura flexible que le permita segregar los datos a nivel regional.
- La transferencia de datos personales a cualquier tercer país (como se define en el Reglamento) siempre debe ser una preocupación importante.
- El acceso (físico y digital) a los datos personales que posee debe mantenerse seguro.
- Considere implementar una solución de administración de usuarios/acceso privilegiado.
- Asegúrese de que incluso los usuarios privilegiados autorizados, incluidos los administradores de bases de datos y sistemas, no puedan acceder a los datos personales en forma clara.
- Utilice múltiples factores de autenticación; considere los autenticadores FIDO; evite SMS como un factor; considere estándares de autorización modernos (y productos que los admitan), incluidos protocolos establecidos como XACML, estándares más nuevos como UMA y enfoques emergentes como la autorización transaccional.
- Tenga cuidado de que los datos personales solo se muestren al usuario correctamente autorizado y que no se puedan almacenar en caché a través de las visitas de diferentes usuarios.
- Tenga especial cuidado para asegurarse de autenticar correctamente al usuario y de que esté debidamente autorizado.
- Evite almacenar información de identificación personal y, en su lugar, solicítela en tiempo real cuando sea necesario tomar una decisión (y verifíquela según sea necesario).
- Si descubre una infracción en su sistema, no envíe datos personales como parte de su informe de infracción.
- Asegúrese de que su sistema tenga un mecanismo de autoservicio para admitir la corrección y/o eliminación de los datos personales de un usuario.
- Considere mantener registros de auditoría para tales transacciones (teniendo en cuenta que querrá mantener los datos personales reales fuera del registro).
- Considere mantener un registro separado que indique cuándo se crearon originalmente los datos en cuestión y ejecute una tarea automatizada para informar sobre los datos que han llegado a su fecha de retención (por lo tanto, marcarlos para su eliminación manual) o para eliminarlos directamente, de acuerdo con su política de privacidad y aviso.
- Verifique antes de una eliminación masiva y requiera autorización adicional para solicitudes que excedan una cierta cantidad de registros.
- Asegúrese de tener una forma de hacer una copia de seguridad de los datos de forma rutinaria y restaurarlos en caso de un error (o un intento deliberado de

corromper los datos), y considere forzar una copia de seguridad a través de su código API antes de que se ejecute el proceso de eliminación.

1 Para una descripción general, lea el artículo RGPD del Cuerpo de conocimiento de IDPro. El texto completo de la Regulación puede ser encontrado en https://eur-lex.europa.eu/eli/reg/2016/679/oj

2 Organización para la cooperación económica y el desarrollo, "El marco de privacidad de la OCDE," 2013, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

3 Puede encontrar una descripción general de la historia del RGPD en https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

4 Naciones Unidas, "La Declaración Universal de Derechos Humanos," 1948, https://www.un.org/en/universal-declaration-human-rights/

5 Organización para la cooperación económica y el desarrollo, "Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales," 2013, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

6 Ver Artículo 25 de la Regulación.

7 KJ Dearie, "¿Qué es el mapeo de datos? La importancia del mapeo de datos para el cumplimiento de RGPD," Termly, 30 octubre 2018, https://termly.io/resources/articles/gdpr-data-mapping/

8 "RGPD: Oficial de Protección de Datos," *Intersoft Consulting*, https://gdpr-info.eu/issues/data-protection-officer/

9 "RGPD: Datos personales," *Intersoft Consulting*, https://gdpr-info.eu/issues/personal-data/

10 "RGPD: privacidad por diseño," *Intersoft Consulting*, https://gdpr-info.eu/art-25-gdpr/

11 Ver en particular el artículo 38 de la Regulación.

12 Ver Artículo 4 de la Regulación.

13 Dearly, "¿Qué es el mapeo de datos? La importancia del mapeo de datos para el cumplimiento de RGPD," https://termly.io/resources/articles/gdpr-data-mapping/

14 Parlamento Europeo, Consejo de la Unión Europea, “Directiva 2009/136/EC del Parlamento Europeo y del Consejo,” noviembre 2009, http://data.europa.eu/eli/dir/2009/136/oj

15 Ver Artículo 9 de la Regulación.

16 Ver Artículo 8 de la Regulación.

17 Ver Artículo 22 de la Regulación.

18 *Greenfield* es un término utilizado para describir un proyecto sin trabajo previo que limite su desarrollo.
Brownfield, por el contrario, refiere a proyectos con limitaciones predeterminadas basadas en tener que trabajar en una plataforma existente o bajo restricciones preexistentes.

19 Especificaciones y Documentos Auxiliares, Grupo de Trabajo de Acceso Administrado por Usuarios, *Kantara Initiative*, https://kantarainitiative.org/confluence/display/uma/Specifications+and+Auxiliary+Documents

20 Lizar, Mark and David Turner, eds. “Especificación de recibo de consentimiento,” Consent & Grupo de trabajo de intercambio de información, *Kantara Initiative* Https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/

21 “Los Principios,” Guía de la Oficina del Comisionado de Información sobre el Reglamento General de Protección de Datos (RGPD), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

22 Katarzyna Szymielewicz, Bill Budington, “El RGPD y las huellas dactilares del navegador: cómo cambia el juego para los rastreadores web más sigilosos,” *Electronic Frontier Foundation*, 19 junio 2018, https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers

23 “Prueba de conocimiento cero,” Wikipedia, última adaptación 24 enero 2020, https://en.wikipedia.org/wiki/Zero-knowledge_proof.

24 “Art. 15 RGPD Derecho de acceso del interesado,” *Intersoft Consulting*, https://gdpr-info.eu/art-15-gdpr/