Una introducción al RGPD (v3)

Por Andrew Cormack, asesor regulatorio principal de Jisc

Para comentar sobre este artículo, visite nuestro repositorio de GitHub y envíe su problema.

Tabla de contenidos

Resumen

El Reglamento General de Protección de Datos (RGPD) se aplica a cualquier procesamiento (incluidos la recopilación, el almacenamiento o el intercambio) de datos relacionados con personas identificables (incluidos números de serie, direcciones IP, etc.) que se encuentran físicamente en Europa.
Este alcance bien puede cubrir las actividades de gestión de acceso e identidad (IAM) internacionales o en línea, así como todas las actividades de IAM realmente realizadas en Europa. Todo ese procesamiento debe cumplir con siete principios: legalidad, equidad y transparencia; limitación del propósito; minimización de datos; exactitud; limitación de almacenamiento; integridad y confidencialidad; responsabilidad. Los individuos tienen derechos de información; derecho de acceso del interesado; rectificación, borrado y

restricción. El procesamiento debe ser por una de las seis bases legales: contrato, obligación legal, intereses vitales, intereses públicos, intereses legítimos o consentimiento. Cada base tiene sus propios requisitos; algunos confieren derechos adicionales a los individuos.

Introducción

El Reglamento General de Protección de Datos (RGPD),[1] que entró en vigor en todos los Estados miembros de la UE el 25 de mayo de 2018, se aplica al procesar "cualquier información relacionada con una persona física identificada o identificable".[2] La inclusión de 'identificable' lo hace mucho más amplio que la mayoría de las leyes de privacidad: las direcciones IP, las direcciones MAC de los dispositivos personales, los números de cuenta e incluso patrones únicos o combinaciones de atributos pueden ser suficientes para incluir una actividad dentro de su alcance. El "procesamiento" no se limita a los formatos digitales: se cubre la información personal preparada para el procesamiento digital o derivada del mismo, así como el contenido de cualquier sistema de archivo estructurado. La gama de actividades cubiertas es igualmente amplia: incluye 'recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición de otro modo, alineación o combinación, restricción, borrado o supresión '.[3] Dado que el RGPD cubre físicamente a todas las personas en Europa (no existe un requisito de ciudadanía o similar), es muy probable que también aplique a las actividades internacionales o en línea de organizaciones en otras partes del mundo, así como a todas las organizaciones en Europa.

Es probable que las actividades de IAM estén reguladas por el RGPD; sin embargo, una IAM efectiva puede facilitar que las organizaciones cumplan con los requisitos de la ley. El comportamiento que prescribe es cada vez más el esperado, no solo en Europa, sino en un creciente número de países que se suscriben al Convenio 108 del Consejo de Europa.[1] Dentro de Europa existen multas significativas por contravenir el RGPD, pero seguir sus principios debería tener beneficios para la reputación y operación eficiente de las organizaciones en cualquier parte del mundo.

Este artículo no es una guía completa del RGPD, pero cubre los aspectos más relevantes para IAM. En primer lugar, describe los principios generales y las obligaciones que se aplican a todo tratamiento de datos personales; luego examina las bases legales permitidas para el procesamiento y las obligaciones y derechos específicos asociados con ellos. Finalmente, los ejemplos muestran cómo las actividades de IAM pueden ayudar a las organizaciones a cumplir con los requisitos del RGPD.

Terminología

- **Ley General de Protección de Datos (RGPD).** Formalmente, Reglamento 2016/679 de la Unión Europea, en vigor desde el 25 de mayo de 2018. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- **Información personal.** Definido en el Artículo 4(1) del RGPD: "'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;". Nota: "persona física" (humano) se utiliza para distinguir de las empresas y otras entidades corporativas que son "personas jurídicas".

- **Procesamiento.** Definido en el Artículo 4(2) del RGPD: "'procesamiento' significa cualquier operación o conjunto de operaciones que se realiza con datos personales o conjuntos de datos personales, ya sea por medios automatizados o no, como la recopilación, el registro, la organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición de otro modo, alineación o combinación, restricción, borrado o destrucción". Tenga en cuenta que incluso esta larga lista de actividades no es definitiva: otras actividades también pueden caer dentro de la definición de "procesamiento". Las reglas adicionales, en el artículo 22, se aplican a la "toma de decisiones individuales automatizadas, incluida la elaboración de perfiles". Estos generalmente tienen el efecto de fortalecer los derechos de información y objeción descritos más adelante y pueden limitar el uso de la automatización para algunas decisiones de alto impacto.
- **Categoría especial de datos.** Categorías de datos que se consideran particularmente sensibles, por lo que están sujetos a una regulación adicional. Definido en el Artículo 9(1) del RGPD como "datos personales que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin de identificar de manera unívoca a un persona, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física"; Los "datos personales relacionados con condenas e infracciones penales" del artículo 10 requieren un tratamiento similar, por lo que normalmente se consideran como otra categoría especial de datos.
- **Controlador de datos.** Según lo definido en el artículo 4, apartado 7, del RGPD: "'controlador' significa la persona física o jurídica, autoridad, organismo u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de datos personales;". Este artículo utiliza el término "organización" como sinónimo de "controlador de datos", ya que las organizaciones involucradas en IAM normalmente serán controladores de datos.
- **Procesador de datos.** Definido en el Artículo 4(8) del RGPD para situaciones en las que una organización procesa datos personales únicamente siguiendo las instrucciones de otros. Un procesador de datos no debe determinar los propósitos del procesamiento, por ejemplo, procesando en su propio interés ni tampoco, más allá de las opciones técnicas limitadas, los medios para hacerlo. Los procesadores de datos están regulados por el Artículo 28: en particular, deben tener un contrato con el controlador de datos que cubra todos los temas enumerados en el Artículo 28 (3). Los Procesadores de datos están excluidos de algunas, pero no de todas, las responsabilidades y deberes de los controladores de datos.
- **Sujeto de datos.** Definido en el Artículo 4 (1) del RGPD (ver "Datos personales" más arriba) como el término formal para el ser humano con el que se relacionan los datos personales. En este artículo se utiliza el término "individuo" como sinónimo de "sujeto de datos".

Reglas para datos personales

El RGPD impone la mayoría de sus obligaciones a las organizaciones que “determinan […] los fines y medios del procesamiento de datos personales” (Art 4(7)): estas organizaciones se denominan *controladores de datos*. Algunas organizaciones pueden procesar datos únicamente en nombre de otros, sin determinar los propósitos y los medios; estos se conocen como *procesadores de dato*s y tienen menos obligaciones. Dado que es probable que los sistemas IAM actúen como controladores de datos, sus principales obligaciones se describen aquí. Las obligaciones fundamentales de todos los *controladores de datos* son actuar de acuerdo con siete principios y satisfacer las obligaciones y los derechos de las personas (*"sujetos de datos"*) cuya información procesan.

Principios (Art. 5)

De acuerdo con el Artículo 5 del RGPD, los siguientes principios se aplican a todo el procesamiento de datos personales:

- **Legalidad, equidad, transparencia:** todo procesamiento debe estar cubierto por una de las seis bases legales establecidas en el RGPD (ver a continuación) y no debe infringir otras leyes ni debe ser engañoso. Cualquier actividad que pueda sorprender a las personas debe explicarse y justificarse, al igual que cualquier efecto adverso en las mismas; las organizaciones deben ser abiertas sobre su procesamiento, en particular a través de los derechos a la información y el acceso a los sujetos que se describen a continuación.
- **Limitación de propósito:** los fines para los cuales se procesa la información deben estar claramente establecidos; la información existente solo se puede usar para nuevos propósitos si, o bien, el nuevo propósito es compatible con los existentes (resumido aproximadamente como 'no sorprendentemente diferente'), si es requerido por ley, o si cada individuo ha dado su consentimiento para el nuevo propósito. Los sistemas IAM deben diseñarse para cumplir un solo propósito y cualquier propuesta para reutilizar sus datos para otros fines debe revisarse para verificar su compatibilidad con ese propósito y con la información proporcionada a los usuarios.
- **Minimización de datos:** los datos y el procesamiento deben ser relevantes para el propósito, suficientes para lograrlo ("adecuados"), pero no excesivos. Los sistemas IAM bien definidos deberían contribuir a la minimización de datos: por ejemplo, los sistemas federados pueden reducir la divulgación mediante el uso de identificadores opacos ("seudónimos") que permiten reconocer a una persona cuando regresa a un sistema, sin identificarla. Los sistemas IAM deben estar diseñados para recopilar, usar y divulgar los datos personales mínimos requeridos para cada función. Si una función se puede entregar con datos anónimos o seudónimos, entonces debería ser así. Esta es la base para la protección de datos por diseño, discutida en el Artículo 25 del RGPD.
- **Exactitud:** Los datos personales deben ser exactos y estar actualizados. Si bien las personas tienen derecho a corregir errores en sus datos (consulte "derecho de rectificación" a continuación), las organizaciones no deben confiar en que lo hagan como la única, o incluso principal, forma de garantizar la precisión. Los sistemas IAM que actúan como una única fuente de verdad para sus organizaciones deberían hacer que la precisión sea significativamente más fácil de lograr; aquellos que no lo

hacen deben ir acompañados de políticas, procesos y flujos de trabajo apropiados para garantizar que su información sea y siga siendo precisa.

- **Límite de almacenamiento [tiempo]:** los datos personales no deben conservarse durante más tiempo del necesario para los fines establecidos. Antes de recopilar datos personales, las organizaciones deben saber y declarar cuánto tiempo los conservarán, ya sea en relación con un período de tiempo fijo (por ejemplo, 'seis meses') o un evento conocido (por ejemplo, 'hasta que te vayas'). Las organizaciones deben tener procesos para garantizar que se implementen los períodos de retención establecidos; al final de ellos, los datos deben eliminarse o anonimizarse. Los fines de archivo, investigación y estadísticas pueden permitir que los datos personales se conserven durante más tiempo, pero sujeto a condiciones específicas en las leyes europeas y nacionales.
- **Integridad y confidencialidad:** las organizaciones deben utilizar controles técnicos y organizativos apropiados para proteger la seguridad de los datos personales. Lo que sea apropiado dependerá de la sensibilidad de los datos y el propósito: es probable que cambie tanto a medida que se disponga de nuevas tecnologías y enfoques de protección como a medida que se manifiesten nuevas amenazas y riesgos. El RGPD impone obligaciones específicas en caso de violación de la seguridad, que se describen a continuación. Los sistemas de IAM deberían ayudar a mantener sus propios datos personales de forma segura y como un componente de los sistemas de control de acceso utilizados para evitar el acceso no autorizado a los datos personales en otras partes de la organización.
- **Responsabilidad:** las organizaciones deben poder demostrar que cumplen los principios y otros requisitos del Reglamento. Esto normalmente requerirá documentación que demuestre que estos principios y requisitos se consideraron en el diseño del sistema, y registros de auditoría (que pueden contener datos personales) que confirmen que las operaciones normales y las respuestas a eventos tales como infracciones y cualquier ejercicio de los derechos individuales se llevaron a cabo, de hecho, de conformidad con ellos.

Derechos y obligaciones

Se aplican tres grupos de "derechos" a todo el procesamiento de datos personales, excepto cuando se aplican excepciones limitadas, establecidas en los artículos específicos. El primer grupo crea una obligación de las organizaciones hacia todos aquellos cuya información procesan; el segundo y el tercero requieren que las organizaciones cuenten con sistemas para atender las solicitudes de las personas que ejercen sus derechos:

- **Derechos de información:** para respaldar los principios anteriores, las organizaciones deben proporcionar al menos un conjunto mínimo de información a todos aquellos cuyos datos personales se procesan: quién es la organización, qué datos se procesan, por qué, durante cuánto tiempo, si se trata de decisiones automatizadas; cualquier otra organización o procesamiento adicional involucrado; cómo ejercer sus derechos. El Artículo 13 se aplica cuando los datos se recopilan directamente del individuo; el Artículo 14 cuando una organización obtiene datos personales de otra fuente (incluidas fuentes públicas).
- **Derecho de acceso del sujeto:** las personas tienen un derecho general, en virtud del Artículo 15, a preguntar y ser informados si sus datos están siendo procesados, qué datos, por qué, durante cuánto tiempo, si se trata de decisiones automatizadas; la fuente de los datos y los destinatarios; cómo ejercer sus derechos. Además, si esto se puede hacer sin afectar los derechos de los demás, el individuo tiene derecho a recibir una copia de sus propios datos. Determinar qué publicar y cuándo puede ser complejo, especialmente cuando la identidad del solicitante puede ser incierta. Los sistemas IAM que fueron construidos en torno a la guía de los reguladores[1] pueden reducir el riesgo de error o fraude.
- **Derechos de rectificación/supresión/restricción:** El Artículo 16 ("rectificación") da derecho a las personas a corregir datos personales inexactos, incluso a agregar información adicional. El Artículo 17 ("borrado") da derecho a las personas a que se eliminen sus datos personales si no existe una base legal para conservarlos. Esto podría surgir, por ejemplo, cuando se retiene demasiada información, si se ha mantenido más allá de su tiempo de retención, o si se estaba procesando sobre la base del consentimiento (ver más abajo) cuando se ha retirado ese consentimiento. El Artículo 18 ("restricción") da derecho a una persona a bloquear el procesamiento posterior de sus datos (incluida la eliminación) mientras se procesa un derecho de rectificación u objeción, o como alternativa a la eliminación si la persona necesita los datos para un reclamo legal. Los sistemas IAM que brindan un único punto de verdad y control deberían facilitar la implementación de estos derechos.

Bases legales para el procesamiento

Para que sea lícita, cualquier actividad que implique el procesamiento de datos personales debe estar cubierta por una de las seis bases legales establecidas en el Artículo 6 del RGPD. Tenga en cuenta que la base se aplica a una actividad de procesamiento en particular, no a un conjunto de datos. Como se ilustra en el ejemplo a continuación, un sistema IAM puede involucrar varias bases legales diferentes. Si bien los profesionales de IAM probablemente

[1] Véase, por ejemplo, el regulador del Reino Unido en: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

no deberían determinar las bases legales en nombre de sus organizaciones, deben ser conscientes de las implicaciones de esa elección.

Varios tipos de datos personales, incluidos la raza, el origen étnico y la salud, se consideran de mayor riesgo y el procesamiento debe ser para uno de los fines establecidos en el Artículo 9, además de basarse en el Artículo 6. Los requisitos para el procesamiento de estos tipos, conocidos como datos de categoría especial, a menudo se establecen en la legislación nacional, en lugar de la europea. Por lo tanto, los sistemas IAM que los procesan deben consultar a abogados familiarizados con los esquemas nacionales pertinentes. Del mismo modo, aunque el RGPD destaca los riesgos adicionales que implican los datos personales de los niños, los requisitos adicionales específicos, incluida la edad por debajo de la cual alguien se considera un niño, se establecen en gran medida a nivel nacional, por lo que no se tratan aquí.

Cada una de las bases del Artículo 6 impone condiciones adicionales al procesamiento, tanto por su definición como, en algunos casos, por adiciones explícitas. Varias de las bases también crean obligaciones adicionales para las organizaciones que procesan datos personales y/o derechos para las personas cuyos datos personales se procesan. Las siguientes secciones describen estas bases legales; aquí se establecen en el orden probable de preferencia de las organizaciones, en lugar de en el que se enumeran en la legislación; los que se encuentran al final de la lista son significativamente más costosos.

Necesario para la ejecución de un contrato

Cinco de las bases legales comienzan con “necesario para…”. Los reguladores han confirmado que esto significa que no debe haber una forma menos intrusiva de lograr el propósito.

La inclusión de “ejecución de” indica que debe existir un vínculo particularmente estrecho entre el procesamiento y el objeto del contrato; la persona cuyos datos se procesan también debe ser parte del contrato. Sin embargo, es probable que el término “contrato” se interprete ampliamente y abarque muchas situaciones en las que las partes han llegado a un acuerdo, incluso sin un documento de contrato formal. Si detener el procesamiento hiciera imposible cumplir con ese acuerdo, entonces "necesario para el contrato" bien puede ser una base adecuada. Es probable que esto se aplique a muchos sistemas IAM, por ejemplo, los proporcionados para uso interno por un empleador o educador. Incluso para los sistemas de IAM independientes, siempre que exista una relación directa entre el individuo y el proveedor de IAM, el uso de "necesario para el contrato" puede ser una forma útil de distinguir los datos y el procesamiento mínimos para que funcione el servicio, de los datos opcionales que el sistema puede usar, pero que no necesita. Este último debe utilizar la base del "consentimiento" que se describe a continuación. Las Directrices de la Junta Europea de Protección de Datos aclaran que es probable que las funciones auxiliares, incluida la mejora del servicio, la prevención del fraude y la publicidad conductual en línea, necesiten un marco legal diferente[2].

[2] Consejo Europeo de Protección de Datos, “Directrices 2/2019 sobre el procesamiento de datos personales en virtud del artículo 6(1)(b) del RGPD en el contexto de la prestación de servicios en línea a interesados”, Versión

Cuando los datos personales se procesan sobre esta base, el RGPD introdujo un derecho a la portabilidad (Artículo 20) que cubre los datos "que [el individuo] ha proporcionado". Por lo tanto, este derecho puede cubrir solo un subconjunto de la información disponible en virtud del derecho general de acceso al sujeto, aunque la información debe proporcionarse "en un formato estructurado, de uso común y legible por máquina". Hasta ahora, los reguladores solo han brindado orientación de alto nivel sobre este derecho,[8] incluida la sugerencia de que CSV podría cumplir con los requisitos de formato, por lo que es probable que se produzcan más desarrollos.

Necesario para el cumplimiento de una obligación legal

Cuando una ley europea o de un Estado miembro requiera que una organización procese datos personales, es probable que esta sea la base legal adecuada. Es posible que esto pueda aplicarse a algunos esquemas nacionales de IAM y a aquellos en sectores industriales regulados, pero de lo contrario es poco probable que sea relevante.

Necesario para proteger intereses vitales

Esta base legal puede aplicarse cuando existe una amenaza para la vida o de lesiones graves. ¡Esperemos que no sea relevante para nuestros sistemas IAM!

Necesario para el desempeño de una tarea realizada en el interés público

Esta base legal se usa típicamente cuando una ley permite el procesamiento para una tarea de interés público, pero no lo requiere. Dado que los esquemas de IAM nacionales y otros establecidos por ley normalmente estarán sujetos a un requisito legal (ver "obligación legal" más arriba), en lugar de un permiso, parece poco probable que sea relevante para los sistemas de IAM.

Esta base otorga a las personas el derecho a oponerse al procesamiento, como se describe en "intereses legítimos" a continuación.

Necesario para los intereses legítimos del controlador o de un tercero

Mientras que las primeras cuatro bases cubren situaciones específicas definidas en la ley, las dos últimas (“interés legítimo” y “consentimiento”) son más flexibles y, por lo tanto, están sujetas a requisitos más costosos para proteger a las personas. Esta base de Intereses legítimos requiere no solo que el procesamiento sea necesario para lograr un propósito específico (el "interés"), sino también que ese interés sea "legítimo" y, únicamente, si los beneficios del procesamiento no son anulados por sus riesgos para las personas. Una actividad de procesamiento puede ser necesaria para un interés legítimo, pero aun así ser ilegal si no puede satisfacer esta prueba de equilibrio.

Sin embargo, el interés legítimo será a menudo la base legal más apropiada para la IAM multilateral, por ejemplo, cuando las afirmaciones de identidad se proporcionen a organizaciones externas como complemento de un contrato para algún otro propósito. Es poco probable que las organizaciones que participan en federaciones, ya sea como

2.0, 8 de octubre de 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

proveedores de identidad, proveedores de servicios, autoridades de atributos u otros, sepan lo suficiente sobre el motivo del usuario que realiza una solicitud en particular para saber si es necesario que haya un contrato o, en cambio, una situación en la que el individuo es capaz de dar su libre consentimiento. En lugar de tratar de comunicar esa información entre varias partes o establecer una red de contratos entre ellas, a menudo es más sencillo considerar el interés de cada organización individual en proporcionar el servicio que la persona, al iniciar un proceso de autenticación o autorización, ha solicitado.

Esta base solo puede utilizarse si “dichos intereses no son anulados por los intereses o los derechos y libertades fundamentales del [individuo] que requieren protección de datos personales” (Artículo 6(1)(f)). Antes de que una organización de IAM considere divulgar (o solicitar) información sobre esta base, debe considerar qué riesgos podrían surgir para el individuo como resultado de esa divulgación. La mención de “derechos y libertades fundamentales” indica que se deben considerar los riesgos más allá de la mera protección de datos. Aunque esto puede parecer oneroso, el proceso a menudo se puede simplificar e implementar en forma de políticas de publicación de atributos, al considerar los tipos de datos involucrados y lo que se sabe sobre las entidades que recibirán la información. La divulgación de un atributo de bajo riesgo a una organización que se ha comprometido (o está obligada por sus propias leyes aplicables) a utilizar dichos datos únicamente para la prestación de servicios podría considerarse un riesgo aceptable, dado que la persona debe haber optado primero por solicitar la autenticación federada para los servicios de esa organización.

Cuando se utiliza la base de intereses legítimos, cada individuo tiene un "derecho a oponerse" en virtud del Art.21. El requisito legal es considerar si la organización tiene “motivos legítimos imperiosos” para continuar con el procesamiento, en cuyo caso puede hacerlo. En la práctica, dado que los sistemas IAM deberían, en cualquier caso, procesar solo la información mínima necesaria para brindar su servicio a los usuarios, una objeción es efectivamente una solicitud para dejar de usar aquellas partes del servicio que se basan en intereses legítimos. Por lo tanto, una organización podría responder a tal solicitud verificando que esa sea, de hecho, la intención del individuo.

Consentir

La única base legal que no contiene la palabra "necesario" es que el individuo haya dado su consentimiento para el procesamiento. Sin embargo, esto está sujeto a condiciones significativas (en el Artículo 7 y los textos expositivos 32, 42 y 43) que probablemente hagan que el consentimiento sea inapropiado para gran parte del procesamiento involucrado en IAM. El consentimiento debe indicarse mediante “un acto afirmativo claro que establezca una indicación libre, específica, informada e inequívoca del acuerdo [del individuo]”; debe ser posible retirar el consentimiento en cualquier momento, tan fácilmente como se dio; el consentimiento no será válido “si el [individuo] no tiene una elección libre o genuina o no puede rechazar o retirar el consentimiento sin perjuicio”. El consentimiento puede usarse cuando un sistema IAM puede contener información adicional, o respaldar otro procesamiento, que no es necesario para su función principal (por ejemplo, apodos), pero en este caso, la persona tiene derecho absoluto a que se elimine esa información adicional, o terminar el procesamiento adicional, en cualquier momento.

Además, se presume que el consentimiento que fuera solicitado por un empleador, autoridad u otra organización con poder similar sobre el individuo, no es libre. El consentimiento no debe solicitarse como condición para prestar un servicio. Las organizaciones que se basan en el consentimiento deben poder demostrar que se obtuvo de acuerdo con estas condiciones. En cuanto al "contrato" anterior, el derecho a la portabilidad se aplica a la información obtenida mediante el consentimiento.

Resumen

Las bases "necesarias" –generalmente contrato, interés legítimo u obligación legal– son más adecuadas para la información necesaria para mantener la relación entre el individuo y el sistema IAM. Con estas, la organización no tiene que preocuparse de si se obtuvo un consentimiento lícito, ni de que pueda ser retirado por capricho. El consentimiento debe reservarse para la información que el sistema IAM puede manejar pero que no necesita: circunstancias que tienen muchas más probabilidades de satisfacer los requisitos para que sea válida. El consentimiento, de acuerdo con el regulador de protección de datos del Reino Unido, debe ser una oferta al individuo para entablar una relación más profunda y de mayor confianza.[3]

Transferencias internacionales

Cualquier transferencia de datos personales de un país dentro del espacio económico europeo a uno fuera (comúnmente conocida como "exportación") requiere su propia base legal. La lista completa de posibles bases se puede encontrar en los Artículos 45-49. En la práctica, y a diferencia de la anterior directiva de protección de datos, normalmente será posible utilizar la misma base legal para las operaciones de IAM internacionales que las realizadas dentro de Europa: las transferencias periódicas de datos personales (por ejemplo, entre una organización cliente y un proveedor de IAM no europeo) normalmente deberían estar cubiertas por un contrato que incluya uno de los conjuntos de cláusulas contractuales tipo;[10] las transferencias ocasionales, *ad hoc* y de bajo riesgo deberían poder utilizar la base de los intereses legítimos; el consentimiento se puede utilizar cuando el individuo es libre de elegir si su información personal se transfiere o no. Los arreglos para transferencias internacionales están sujetos a cambios: por ejemplo, tanto el esquema original de puerto seguro de EE. UU. como el escudo de privacidad que lo reemplazó han sido declarados inválidos por el Tribunal de Justicia de la Unión Europea; el último caso ("Schrems II") también agregó nuevas obligaciones para las organizaciones exportadoras que utilizan las cláusulas contractuales estándar: la Comisión Europea emitió nuevas versiones de las cláusulas en junio de 2021.[11] Las organizaciones que operan sistemas IAM internacionales deben estar al tanto de los desarrollos.

Seguridad

Además de exigir a las organizaciones que tomen medidas proactivas para proteger la seguridad de los datos personales, el Artículo 33 del RGPD introduce importantes requisitos de notificación cuando una organización se percata de una "violación de la seguridad que conduce a la destrucción, pérdida, alteración, destrucción, pérdida, alteración, uso no

[3] "¿Cuándo es apropiado el consentimiento? Oficina del Comisionado de Información, consultado el 10 de octubre de 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/#when3.

autorizado, accidental o ilegal, divulgación o acceso a datos personales transmitidos, almacenados o tratados de otro modo". La amplia definición de "violación" y la inclusión de "accidental" significa que las organizaciones deben tener especial cuidado al diseñar, probar y documentar procesos que puedan alterar, eliminar o divulgar datos. Todas estas infracciones deben ser informadas al regulador a menos que sea "poco probable que resulten en un riesgo para los derechos y libertades de las personas físicas". La pérdida de una tarjeta de memoria cifrada, si la clave de descifrado permanece segura, es usada frecuentemente como un ejemplo de una infracción que puede no ser necesario informar. La expectativa es que dichos informes se envíen dentro de las 72 horas: de lo contrario, se debe incluir una explicación satisfactoria de la demora. Cuando es probable que una violación implique un "alto riesgo" para los derechos y libertades de las personas, se requiere una notificación a las personas afectadas en virtud del Artículo 34.

El RGPD reconoce en el texto expositivo 49 que la capacidad de detectar, contener y remediar las infracciones de seguridad es una parte importante para mantener la seguridad de los datos. De hecho, se ha sugerido que el hecho de no hacerlo puede ser en sí mismo una infracción al Artículo 33. El procesamiento de datos personales, como los registros de acceso y actividad necesarios para esos fines, se reconoce como un interés legítimo (así permitido, sujeto a la prueba de ponderación). Estos registros deben, por supuesto, mantenerse y procesarse de forma segura. IAM puede desempeñar un papel importante en la mitigación de las infracciones de seguridad, al deshabilitar las cuentas comprometidas de manera rápida y efectiva; sus registros también pueden proporcionar una alerta temprana cuando una organización está bajo ataque.

Para cumplir con el ajustado cronograma del RGPD para comprender y reportar infracciones, las organizaciones deben planificar, preparar, asignar recursos y practicar cómo responderán a los incidentes de seguridad. Esto podría incluir evaluar qué tipos de incumplimiento del sistema IAM requerirían notificación a los reguladores, individuos o a ninguno, así como identificar y establecer contacto con los socios internos y externos cuya ayuda sería necesaria.

Ejemplos de gestión de identidades y accesos

Los siguientes ejemplos muestran formas en que los sistemas IAM pueden admitir el RGPD.

Ejemplo 1: Sistemas de oficina subcontratados

John trabaja en una pequeña empresa, que ha contratado a un proveedor de servicios en la nube para ejecutar sus servicios de *software* de oficina y recursos humanos. Según lo acordado en dicho contrato, el proveedor de servicios subcontrata la operación de intercambio de correo electrónico y documentos a Google. El empleador de John ingresa la información necesaria para su función laboral en una serie de formularios web; el proveedor de servicios configura las cuentas necesarias y los permisos de documentos. Los datos personales de John se procesan sobre la base de que son necesarios para su contrato de trabajo; solo se pasa a Google la información necesaria para configurar su cuenta de correo electrónico y documentos.

En este ejemplo, John es el sujeto de datos y su empleador es el controlador de datos. Siempre que únicamente utilicen la información para prestar los servicios contratados, el prestador del servicio y Google son encargados del tratamiento. Si alguno de ellos utilizara los datos para sus propios fines, por ejemplo, para mostrar anuncios personalizados, entonces sería el controlador de datos para ese procesamiento y estaría obligado a cumplir con todas las obligaciones del controlador de datos.

Ejemplo 2: Gestión de acceso federado

Janet es profesora en la Universidad de Erewhon. La universidad tiene un sistema IAM central que contiene los detalles de todo el personal necesario para realizar su trabajo. Esta información se almacena y procesa sobre la base legal de que es necesaria para el contrato de trabajo de Janet con la universidad: sin hacerlo, sería imposible cumplir con ese contrato. El sistema IAM actúa como un único punto de verdad, lo que garantiza que la información esté actualizada en toda la universidad y que cualquier solicitud de corrección se pueda implementar fácilmente.

El sistema IAM también le permite a Janet almacenar información opcional, como sus intereses personales, que aparecerán en la página web de su personal. Dado que puede agregar, cambiar o eliminar estos en cualquier momento, sin afectar su trabajo, la base legal adecuada es el consentimiento.

La universidad también es miembro de una Federación de Infraestructura de Autenticación y Autorización (AAI, por sus siglas en inglés). Cuando Janet accede a un sitio web de otro miembro de la Federación (por ejemplo, el editor de una revista), puede optar por iniciar sesión con sus credenciales universitarias. Una amplia variedad de organizaciones son miembros de la Federación ya que, siendo la universidad la responsable de proporcionar información verificada y velar por el buen comportamiento de sus usuarios, esto les permite recibir y procesar muchos menos datos personales, de acuerdo con el principio de minimización de datos. Janet necesita acceder a algunos de estos por su trabajo, pero otros pueden ser solo por interés personal. Dado que ni la universidad ni los sitios desean determinar qué sitios son necesarios para el contrato y a cuáles se accede con consentimiento libre (cuando Janet necesita acceder a un sitio para trabajar, su consentimiento no puede ser libre), ambos usan la base legal de que el procesamiento es necesario en su interés legítimo de ayudar a Janet a acceder a la información que desea.

La base de los intereses legítimos requiere que la universidad equilibre los riesgos de divulgar información con los beneficios. Dado que el acuerdo de la federación requiere que los miembros utilicen únicamente la autenticación y otros atributos con fines de prestación y personalización del servicio, y que no intenten identificar a los usuarios seudónimos, la universidad evalúa que existe muy poco riesgo al divulgar un identificador opaco único y el estado de Janet como un miembro del personal de cualquier miembro de la Federación; por lo tanto, ha configurado sus sistemas para publicar esa información de forma predeterminada cuando un usuario solicita un inicio de sesión federado. Esto es suficiente tanto para que Janet acceda a las revistas en línea como para comprobar su derecho a un descuento para el personal en el gimnasio local.

La Federación ha definido una clase de servicios que están diseñados específicamente para uso en investigación y educación, y que requieren un nombre y una dirección de correo electrónico además del identificador y el estado opacos. Este requisito adicional se menciona en los avisos de privacidad de los servicios. Si bien esta divulgación implica un riesgo ligeramente mayor, la universidad está satisfecha de que esto se justifique por el mayor beneficio; por lo tanto, tales servicios recibirán la información adicional por defecto. Esto le permite a Janet usar grupos de discusión y entornos de investigación virtuales en su campo.

Cuando los servicios soliciten más información, la universidad realizará una evaluación individual del beneficio y el riesgo. Esto puede indicar que se requieren medidas adicionales, como un contrato bilateral o el libre consentimiento de cada individuo, para reducir el riesgo de divulgación.

En este ejemplo, Janet es el sujeto de datos. Tanto la universidad como el proveedor de servicios son controladores de datos, ya que el proveedor de servicios elige qué servicios ofrecer a Janet.

Biografía del autor

Andrew Cormack es el principal asesor regulatorio de Jisc. Ha estado involucrado en el desarrollo técnico y de políticas de los sistemas de identidad federada en el Reino Unido, Europa y en todo el mundo durante más de quince años. Ha hablado y escrito de forma extensa sobre cómo se pueden utilizar las tecnologías digitales para mejorar la privacidad y la protección de datos y, más recientemente, sobre la aplicación del RGPD a las mismas. Sus publicaciones se pueden encontrar en https://orcid.org/0000-0002-8448-2881 y sus blogs en https://community.jisc.ac.uk/blogs/regulatory-developments.

Registro de cambios

Fecha	Cambios
2021-06-30	Actualizado en base a https://github.com/IDPros/bok/issues/42, https://github.com/IDPros/bok/issues/41
2022-09-30	Información actualizada sobre las cláusulas contractuales tipo de la UE