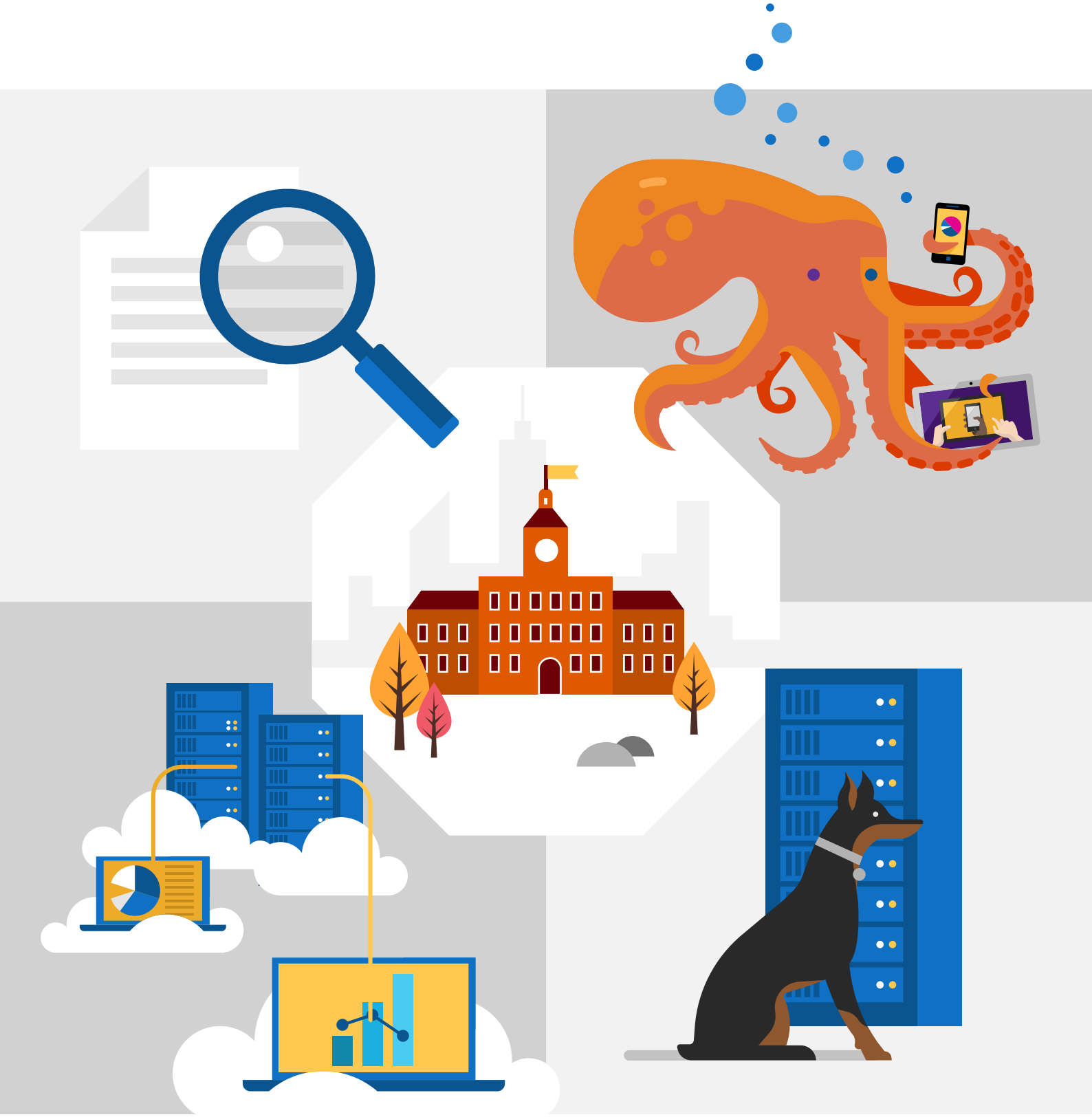


El RGPD (Reglamento General de Protección de Datos) para instituciones docentes

Una guía de inicio para instituciones docentes

Microsoft

Acerca de esta guía

Esta guía ha sido concebida para ayudarle con el cumplimiento del nuevo Reglamento General de Protección de Datos (RGPD) e incluye ejemplos concretos y listas de tareas. No se trata de una guía exhaustiva, sin embargo, le brinda una visión general de los procesos y factores que deben tenerse en cuenta a partir del 25 de mayo de 2018, cuando el RGPD entra en vigor.

El RGPD es de aplicación para instituciones con presencia física en la UE, además de para organizaciones que proporcionan productos y servicios a los ciudadanos de la UE o que reúnen y analizan datos asociados con residentes en la UE. Si su institución reside fuera de la UE, considere esta guía de cumplimiento del RGPD como un modelo de la mejor práctica.

La docencia es una historia de datos

Al comienzo de todos los años académicos, los nuevos estudiantes producen enormes cantidades de datos en escuelas y universidades. Esto se suma a las montañas de datos que estas organizaciones ya gestionan como propietarios de datos.

Sin embargo, estos datos son vitales para el funcionamiento de escuelas y universidades. Por lo tanto, es necesario tener implantados procesos claros y bien documentados para todos y cada uno de los registros tramitados.

Además, estos procesos necesitan extenderse más allá del tiempo que un estudiante pasa en la institución. Cuando dejan la institución, es necesario contar con políticas documentadas para la protección, retención y tratamiento de bases de datos, archivos e incluso mensajes de correo electrónico.

Definiendo el viaje de los datos

La información producida y procesada en las instituciones docentes sirve diversos propósitos.

Primero está el plan de estudios, los conocimientos que los educadores comparten con los estudiantes, reforzados por las ideas que los estudiantes generan a medida que progresan a través de su viaje de aprendizaje.

También existe un segundo conjunto de datos: la información que las organizaciones reúnen sobre profesores y estudiantes, además del desempeño del colegio. Si a esto añadimos la información recopilada en los procesos administrativos, procedente de padres, enfermeras escolares, la junta escolar, asesores y agencias externas, contaremos con una fuente de datos aparentemente interminable a través de toda la organización, una gran proporción de los cuales son datos personales.

Como bien saben todos los administradores, este segundo grupo de datos es tan vital para cualquier institución docente como la propia misión docente. Se transforma en parte del viaje RGPD que los estudiantes, profesores y padres emprenden a medida que acceden y comparten información a través de las herramientas de aprendizaje y servicios de comunicación que ofrecen universidades y escuelas.

¿Qué hacer con todos estos estos datos?

Como propietarios de los datos ya estamos sujetos a la legislación existente que exige la manipulación y el tratamiento cuidadoso de los datos que poseemos y gestionamos. Aunque al amparo del RGPD existen consideraciones adicionales sobre cómo, por qué y con quién necesitamos compartir parte de estos datos con organizaciones tales como organismos reguladores y estatales, además de con terceros como proveedores de seguros, que los procesan y analizan, lo más probable es que ya tengamos implantadas múltiples políticas de protección de datos y privacidad.

Sin embargo, ¿son éstas suficientes para proteger la información personal y sensible que manipulamos?

Introducción del RGPD

A partir del 25 de mayo de 2018, muchas organizaciones, incluso aquellas fuera de la Unión Europea (UE), serán responsables de todos los datos que mantienen al amparo de una nueva legislación, a saber, el Reglamento General de Protección de Datos (RGPD).

Esta legislación ha sido concebida para proteger la privacidad de los datos de todos los ciudadanos de la UE, al tiempo que armoniza la legislación existente en materia de privacidad de datos en Europa. El RGPD tendrá impacto sobre los datos que poseemos, cómo los usamos, dónde los guardamos y durante cuánto tiempo podemos conservarlos.

¿Por qué es importante el RGPD?

El viaje de una institución docente puede reflejar el viaje de aprendizaje de un estudiante, marcado por piedras angulares que se registran y evalúan en todas las etapas del camino. Algunas veces, los datos producidos permanecerán sin cambios durante años, mientras que otras podrán cambiar rápidamente a medida que tanto los estudiantes como el personal docente se mueven a través de la institución.
El RGPD crea un marco de trabajo legal uniforme para toda Europa, ofreciendo a las personas físicas que residen en Europa derechos sobre sus datos personales.

Los principales cambios que afectan al sistema docente incluyen:

Privacidad personal

Las personas tiene derecho a:

- Acceder a sus datos personales
- Corregir errores en sus datos personales
- Eliminar sus datos personales
- Objetar al tratamiento de sus datos personales
- Exportar sus propios datos personales

Controles y avisos

Necesitará:

- Proteger los datos personales utilizando la seguridad apropiada
- Notificar a las autoridades de las filtraciones de los datos personales
- Documentar cómo procesamos los datos personales
- Mantener registros que detallen el tratamiento de los datos y el consentimiento*

Políticas transparentes

Se espera que:

- Comuniquemos claramente la recogida de datos
- Detallemos los fines del tratamiento y los casos de uso
- Definamos las políticas de retención y eliminación de los datos
- Detallemos cómo los clientes pueden ejercer sus derechos al amparo del RGPD

Informática y formación

Las instituciones docentes necesitarán:

- Ofrecer formación al personal docente y a los empleados que tratan con la privacidad como administrativos o personal informático
- Auditar y actualizar las políticas relacionadas con los estudiantes, personal y contratistas
- Contratar a un Responsable de Protección de Datos (si fuera necesario)
- Crear y gestionar el cumplimiento de los contratos de vendedores, incluyendo todos los vendedores y profesores suplentes

***El RGPD incluye protecciones especiales para los niños. En general, especifica que el consentimiento de los niños debe ser "explícito". El RGPD establece la edad de consentimiento, en el contexto online, a los 16 años. Sin embargo, los estados Miembros de UE podrían establecer individualmente la edad de consentimiento entre los 13 y los 16 años.**

¿Cómo le afecta a usted el RGPD?

¿Cómo podemos alinear estas nuevas normas con el hecho de que en una institución son muchas las personas que necesitan acceder a los datos todos los días?

El RGPD ofrece el reglamento para gestionar y proteger estos datos al tiempo que crea políticas y prácticas consistentes. Depende de usted afianzar un marco de trabajo en el que el RGPD funcione para su institución.

Derechos más amplios para la privacidad personal

El RGPD refuerza la protección de los datos de las personas, incluyendo estudiantes, dentro de la UE, asegurando que tengan derecho a:

- Acceder a los datos y corregir errores
- Eliminar datos
- Objetar al tratamiento de su información
- Mover sus datos

Mayor obligación de documentar los procesos y proteger los datos

Las instituciones docentes que tramitan datos personales necesitarán demostrar evidencia clara de cumplimento.

Notificación obligatoria de filtraciones de los datos personales

Las instituciones docentes tienen la obligación de informar de las filtraciones de los datos personales en un plazo de 72 horas.

Multas considerables por incumplimiento

Las instituciones docentes se arriesgan a tener que pagar posibles multas si no responden. Para cumplir el reglamento es importante tener en cuenta varias medidas para proteger los datos personales y ser precavido a la hora de manipularlos.

¿Cómo empezar?
Mapa de cumplimiento del RGPD

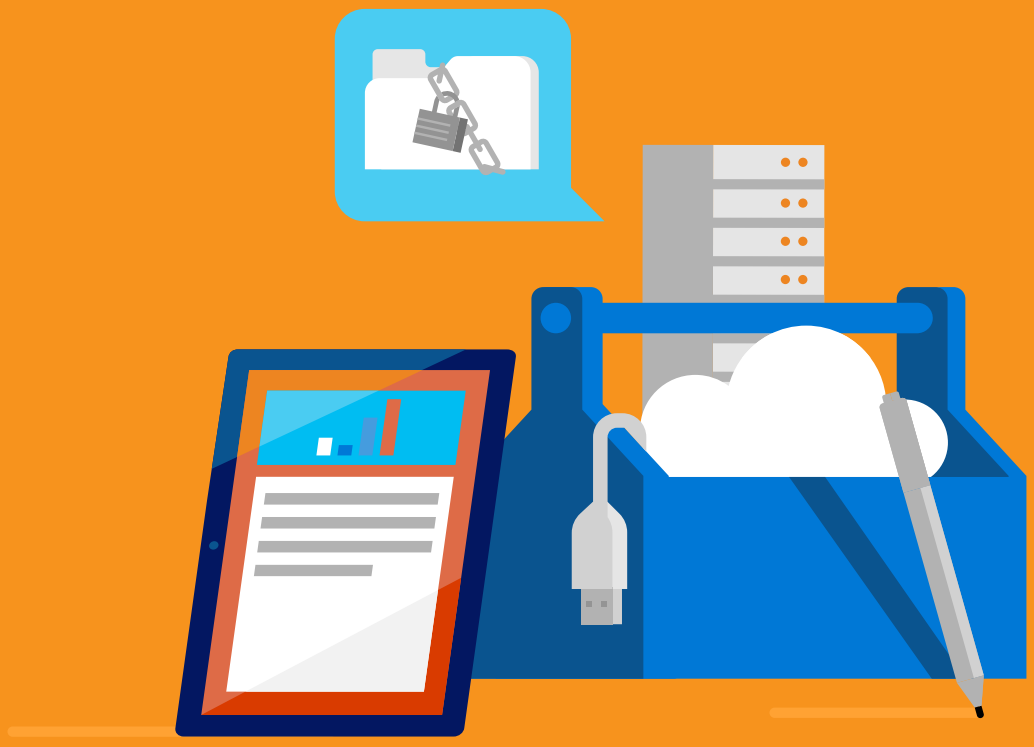
El RGPD tendrá un gran impacto para su institución ya que requiere la actualización de las políticas de privacidad personal, así como la implementación o fortalecimiento de los controles de protección de los datos y procedimientos de notificación de filtraciones de los datos personales, además del despliegue de políticas transparentes y la inversión adicional en sistemas informáticos y formación.

Gracias al exhaustivo conjunto de productos de cumplimiento de cualquier proveedor de servicios en la nube, Microsoft Cloud puede facilitar su viaje hacia el cumplimiento del RGPD. Descubrirá que Microsoft Cloud le ofrece los recursos que necesita para cumplir con los requerimientos del RGPD.

Hemos desarrollado un proceso para la implementación del RGPD, que se concentra en cuatro etapas claves:

- **Descubrir.** Identificar los datos personales que tiene y dónde están
- **Gestionar.** Controlar cómo se utilizan y accede a los datos personales
- **Proteger.** Establecer controles de seguridad para prevenir, detectar y responder a vulnerabilidades y filtraciones de los datos personales
- **Informar.** Mantener la documentación requerida y gestionar las solicitudes y las notificaciones de filtraciones de los datos personales

Las herramientas y los recursos de Microsoft pueden ayudarle a implementar todas las etapas de cumplimiento del RGPD.



Descubrir

Gestionar

Informar

Proteger

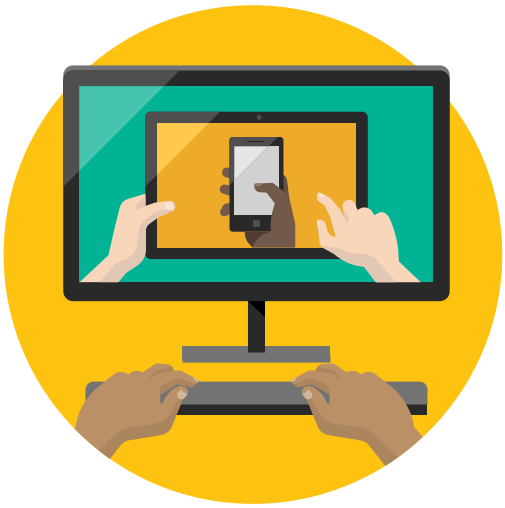
Descubrir

Identificar los datos personales que tiene y dónde están.

Descubrir los datos que tenemos

A menudo los datos personales se guardan en múltiples ubicaciones que incluyen correos electrónicos, documentos, bases de datos, soportes extraíbles, metadatos, archivos históricos y copias de seguridad.

La primera tarea es identificar dónde se reúnen y guardan los datos personales.



Datos existentes

El desafío

Además de guardar y garantizar la seguridad de los datos existentes de forma compatible con el RGPD, también deberíamos documentar el tratamiento que damos a los datos personales, p. ej. 1. consentimiento, 2. contratos, 3. Marco legal, 4. salud, 5. común, 6. causa legítima.

Qué hacer

- Identificar qué datos personales existentes se reúnen y guardan.
- Descubrir las ubicaciones donde se guardan los datos. Asegurarse de incluir a vendedores en la nube y servicios externos de hosting, como páginas web y centros de servicios compartidos. Sin olvidarnos de los datos analógicos, como ficheros que se archivan en archivadores.
- Organizar y etiquetar las bases de datos existentes por carácter confidencial, uso, propiedad, administradores y usuarios.
- Documentar las razones para tramitar estos datos conforme al RGPD
- Verificar los procedimientos de consentimiento y renovarlos cuando corresponda.

Dispositivos y ubicaciones existentes

El desafío

Con frecuencia los datos personales se guardan y se accede a ellos desde una amplia gama de dispositivos. Estos dispositivos pueden incluir servidores, ordenadores de sobremesa y portátiles, tabletas, teléfonos inteligentes, ordenadores domésticos y entornos en la nube no gestionados.

Los dispositivos personales y móviles presentan un desafío especial para el descubrimiento de los datos.

Qué hacer

- Hacer un inventario y enumerar todos los dispositivos en los que podrían guardarse los datos personales.
- Auditar el personal y los dispositivos móviles que no pertenecen a la institución.

Requerimientos del RGPD

El RGPD requiere que todas las organizaciones identifiquen los datos existentes y dónde se guardan.

Una vez de haber creado un inventario de todos los datos, incluyendo ubicaciones, dispositivos y usuarios, pueden establecerse los sistemas para reunir datos nuevos a medida que estos llegan.

Usuarios existentes

El desafío

El RGPD impone estrictas normas sobre quién puede tramitar qué datos y cómo y cuándo pueden hacerlo. Antes de compartir datos personales, necesitará asegurarse que aquellos que tienen acceso a los mismo tienen derecho a verlos, tanto dentro como fuera del entorno escolar.

Qué hacer

- Identificar y enumerar a los usuarios, incluyendo estudiantes, personal y todos los contratistas que podrían tener acceso a estos datos.

Subcontratistas existentes

El desafío

Los datos personales solamente deberían compartirse con o accederse a ellos por las personas autorizadas. Esto es de aplicación tanto a partes internas de la organización como a partes externas. Pensemos en todos los contratistas, incluyendo servicios de catering y limpieza y asistentes externos, que trabajan con la institución.

Es su responsabilidad asegurarse de que las personas autorizadas a acceder a los datos, que al amparo del RGPD se denominan procesadores, cumplan la legislación. Esto significa que deberán guardar los datos personales de forma segura, utilizarlos únicamente con los fines para los que se solicitaron y eliminarlos cuando dejen de necesitarse.

Qué hacer

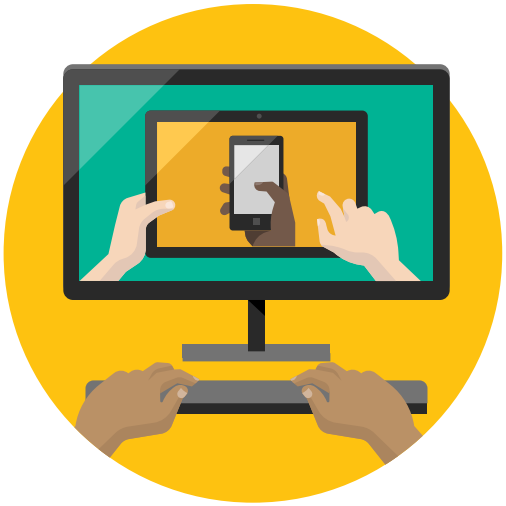
- Identificar y enumerar a todos los subcontratistas en el directorio de usuarios.
- Verificar el cumplimiento del RGPD.
- Firmar un contrato de cumplimiento del RGPD.
- Verificar si puede accederse a los datos desde una ubicación central mientras están en las instalaciones.

Gestionar

Controlar cómo se utilizan
y accede a los datos personales

Gestionar los datos personales

El primer paso a la hora de gestionar datos personales es definir por qué necesitamos reunirlos en primer lugar. Preguntémonos, cómo nos ayudan a ofrecer la docencia. Consideremos cómo deberían reunirse, dónde los guardaremos, qué entidades apoyarán ese proceso, quién debería tener acceso a ellos y cómo habilitaremos los cambios y la eliminación de los mismos.



Gestionar datos nuevos

El desafío

El RGPD permite el uso de los datos necesarios para cumplir su misión. Si esta misión está claramente definida la necesidad de tramitar datos personales asociados con dicha misión aumentará.

Cuando los estudiantes se matriculan, querrá ser transparente sobre los datos personales que ha reunido la institución. Sobre todo, necesitará saber por qué son necesarios estos datos, durante cuánto tiempo los guardará, dónde los guardará y cómo tanto usted como otros accederán a ellos. Cuando corresponda, será necesario solicitar y obtener el consentimiento debido y conservarlo como evidencia.

Los estudiantes menores de edad necesitarán contar con el consentimiento paterno. Cuando contrate a personal, necesitará proporcionar información clara sobre el tratamiento que recibirán los datos.

Qué hacer

- Definir su misión claramente.
- Enumerar a los interesados.
- Establecer los datos personales requeridos.
- Automatizar la recogida de datos y ser responsable de sus acciones.
- Aclarar las cláusulas del RGPD que incluirán los contratos con su equipo de RR HH y verificar el consentimiento y renovar los procesos, cuando sea relevante.

Gestionar dispositivos

El desafío

En un entorno docente, los dispositivos utilizados son diversos y están diseminados a través de una amplia gama de usuarios. Podemos ver los ordenadores domésticos de los profesores, los teléfonos inteligentes y las tabletas de los estudiantes, los ordenadores de las aulas, dispositivos personales, aplicaciones privadas, ubicaciones y aplicaciones en la nube no supervisadas, dispositivos de subcontratistas, llaves USB y ficheros de papel guardados en archivadores.

Para cumplir las estrictas normas del RGPD sobre la seguridad de los datos personales, necesitará gestionar los dispositivos, además del personal docente, estudiantes y contratistas, de forma consistente.

Qué hacer

- Desarrollar políticas sobre el uso de dispositivos.
- Educar al personal y a los estudiantes y sensibilizarles sobre el RGPD.
- Auditorías y eventos de registro.

Los requerimientos del RGPD

El RGPD regula la forma en la que se utilizan y se accede a los datos personales.

Gestionar usuarios

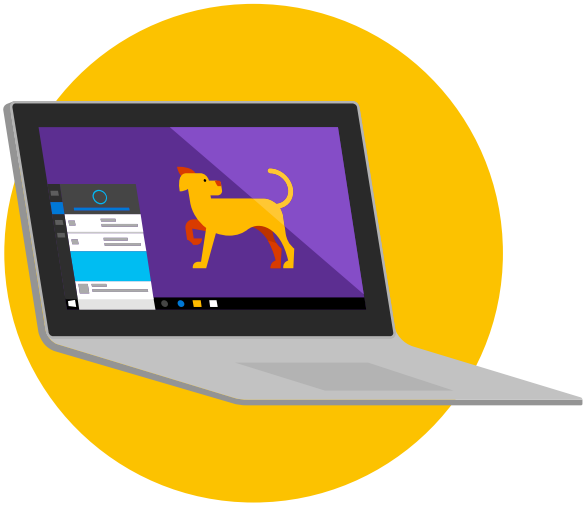
El desafío

Mientras que el proceso de descubrimiento nos ofrece información sobre la base de datos de nuestros usuarios, el proceso de gestión nos ayuda a organizar a los usuarios en listas inteligentes, lo que nos permite establecer los permisos, hacer seguras las políticas de acceso al sistema y seguir la pista de quién accede a los datos.

Cuando los usuarios dejan la institución, es necesario denegar rápidamente el acceso a los recursos escolares con el objeto de evitar posibles filtraciones de información.

Qué hacer

- Organizar a los usuarios en grupos de seguridad.
- Definir permisos y políticas.
- Desplegar las políticas.
- Educar a estudiantes, personal y contratistas sobre el uso correcto de los datos.



Gestionar su página web

El desafío

Las actividades online son una parte vital de las actividades promocionales para atraer a personal y estudiantes. Es su deber asegurar la seguridad de las plataformas online que se utilizan en la institución.

Qué hacer

- Auditar los datos que reúne su página web automáticamente.
- Enumerar las cookies de primeros y terceros.
- Verificar la seguridad terminal a terminal de los formularios electrónicos.
- Verificar que los procesos de consentimiento cumplen el RGPD.
- Producir una declaración de privacidad que documente:
  - La información que se está recogiendo
  - Quién la está recogiendo
  - Cómo se está recogiendo
  - Por qué se está recogiendo
  - Cómo se utilizará
  - Con quién se compartirá
  - Qué efecto tendrá para la persona en cuestión
  - Si el uso propuesto hará que la persona presente objeciones o quejas object or complain

Proteger

Establecer controles de seguridad para prevenir, detectar y responder a vulnerabilidades y filtraciones de los datos personales

Proteger a los usuarios, los datos y los dispositivos

La seguridad es uno de los principales puntos de atención en nuestro moderno mundo informatizado.
Los requerimientos del RGPD incluyen protección física, seguridad de la red, seguridad a la hora de guardar los datos, seguridad de los sistemas informáticos, gestión de la identidad, control de acceso, codificación y mitigación del riesgo. Examinemos cómo supervisamos los sistemas, identificamos las filtraciones, calculamos el impacto de cualquier violación y la forma en la que respondemos y nos recuperamos de las mismas.

Datos

El desafío

El RGPD no es un destino sino un viaje continuo. Requiere que seamos responsables de nuestras acciones en todo momento, que reaccionemos con rapidez cuando sea necesario y que protejamos los datos personales a medida que se abren camino por la institución.

Qué hacer

- Codificar los datos y los correos.
- Proteger los datos en los dispositivos (MAM).
- Guardarlos de forma segura.
- Añadir derechos a archivos y correos individuales.
- Supervisar intrusiones, infecciones, robos y el comportamiento fuera de lo normal.

Dispositivos, ubicaciones y aplicaciones

El desafío

Los dispositivos y las aplicaciones tocan casi todos los aspectos de los datos. Pueden formar parte de la red de área local (LAN), dispositivos móviles, dispositivos en otras ubicaciones como viviendas o campus además de dispositivos y aplicaciones en la nube. Cada dispositivo y aplicación requiere atención específica.

Qué hacer

- Proteger la LAN con antivirus, firewall y protección física.
- Codificar dispositivos, discos y llaves USB.
- Educar a estudiantes y personal sobre la mejor práctica en materia de ordenadores domésticos.

Requerimientos del RGPD

El RGPD establece las directrices necesarias para establecer controles de seguridad para prevenir, detectar y responder a las vulnerabilidades y filtraciones de los datos personales.

Usuarios

El desafío

Una vez que se han definido los usuarios y organizado en grupos de seguridad con permisos y políticas definidos, podemos añadir medidas de protección adicionales como control de acceso y gestión de identidad, para cumplir el RGPD.

Qué hacer

- Analizar las políticas de contraseñas y opciones de acceso al sistema.
- Educar y crear conciencia.

Pruebas

El desafío

Una vez de haber implantado las medidas técnicas y organizativas para proteger los datos personales, será necesario ponerlas a prueba regularmente, evaluar y valorar su efectividad al objeto de asegurar que son adecuadas y apropiadas.

Qué hacer

- Facilitar pruebas regulares.
- Evaluar la eficacia de las medidas de seguridad

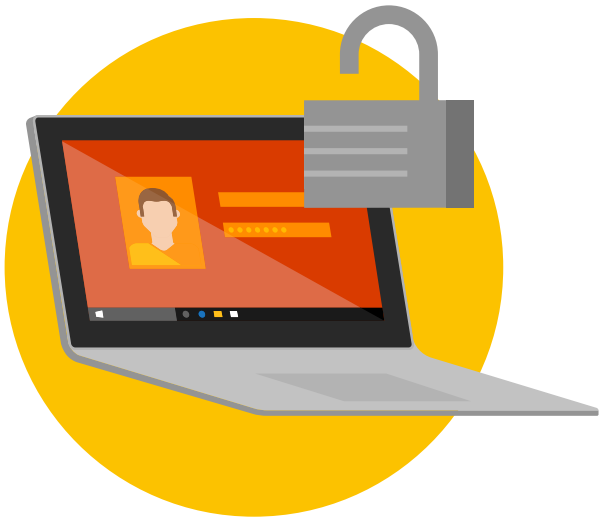
Informar

Mantener la documentación requerida y gestionar las solicitudes y las notificaciones de filtraciones de los datos personales.

Informar sobre auditorias y filtraciones de los datos

Uno de los principios claves de RGPD es ser responsable de nuestras acciones, para ello tendremos que crear itinerarios de auditorías para el tratamiento, clasificaciones y terceros con acceso a los datos personales, incluyendo medidas de seguridad organizativas y técnicas, además de retención de los datos. Es posible que necesitemos realizar Evaluaciones de Impacto sobre la Protección de Datos (EIPD).

Una EIPD requiere que las organizaciones identifiquen y analicen el impacto de una actividad de tratamiento propuesta sobre la protección de datos personales.



Itinerarios de auditorias

El desafío

El RGPD requiere que seamos responsables a la hora de proteger y tramitar los datos personales en la forma apropiada. Los registros deberían incluir la naturaleza de todas las solicitudes que hace una persona, por ejemplo, para ver o rectificar los datos personales, así como la consiguiente resolución.

Qué hacer

- Conservar registros de las solicitudes de datos de las personas para demostrar que cumplimos los requisitos del RGPD.
- Hacer un seguimiento de las salidas y entradas de datos personales de la UE.
- Hacer un seguimiento y registrar los datos enviados a proveedores de servicios externos, como contratistas de servicios de informática o servicios docentes.
- Mantener itinerarios de auditorías para demostrar el cumplimiento del RGPD.
- Hacer un seguimiento y registrar las salidas de datos personales a proveedores de servicios externos.
- Facilitar las Evaluaciones de Impacto sobre la Protección de Datos.

Filtraciones de los datos personales

El desafío

Las organizaciones necesitarán notificar a las autoridades aplicables en un plazo de tiempo de 72 horas de la identificación de filtración de datos personales.

Qué hacer

- Activar registros e informes.
- Responder en el marco de tiempo requerido.
- Mantener un registro separado de cambios a los datos personales en caso de producirse desastre y restauraciones de copias de seguridad.

Requerimientos del RGPD

Las organizaciones necesitarán notificar a las autoridades aplicables en un plazo tiempo de 72 horas de la identificación de filtración de datos personales.

Conclusión

La confianza es fundamental para la misión de Microsoft de atribuir poderes a todas las personas y organizaciones del planeta para que alcancen su máximo potencial. En ningún lugar es esto tan importante como en las instituciones que preparan a la próxima generación de estudiantes para encontrar y cumplir su propósito en la sociedad.

Microsoft está comprometido con sus principios de confianza en la nube – en cuanto a seguridad, privacidad, transparencia y cumplimiento. A medida que el RGPD entra en vigor el 25 de mayo de 2018 la amplia cartera de servicios en la nube de Microsoft, trata las rigurosas demandas de seguridad y privacidad de nuestros clientes docentes, al tiempo que aseguran que cumplimos nuestras obligaciones como procesadores de datos.

El servicio de productividad en la nube de Microsoft, Office 365 A1 es gratis para todos los clientes docentes y ofrece herramientas esenciales para el cumplimiento del RGPD y para la protección de la información, habilitando eDiscovery, gestión de derechos, prevención de pérdida de datos, codificación, capacidades avanzadas de archivado de correos electrónicos y retención legal. Los clientes que requieran análisis de riesgos mejorado, mitigación de amenazas, codificación y control de los datos pueden tener en cuenta planes de pago para Office 365 A3 o A5 para respaldar sus requerimientos RGPD específicos.

Aquellos clientes interesados en soluciones que gestionen archivado de datos, control y descubrimiento para su estado informático más amplio pueden valerse de Microsoft 365 Education. Este producto proporciona una experiencia segura y sencilla para gestionar usuarios, datos y dispositivos desde un único tablero que protege la identidad, las aplicaciones, los datos y los dispositivos con seguridad inteligente mejorada por machine learning.

Empiece hoy mismo utilizando la herramienta GDPR Assessment para evaluar su nivel general de preparación. Y si ya es cliente de Microsoft Cloud utilice Compliance Manager para obtener una visión holística de su posición de protección de datos y cumplimiento para Office 365, Dynamics 365 y Azure.

Herramientas y enlaces asociados

Para ayudarle en su viaje a través del RGPD nos complace ofrecerle el siguiente listado de herramientas.

Descubrir

- Office 365 **Advanced eDiscovery** o **Content Search** le ayudarán a la hora de buscar información existente.
- **Office 365 data labelling** permite clasificar los datos a través de toda la organización para su control.
- **SharePoint Lists** es una herramienta flexible que le ayudará a organizar y etiquetar datos.
- **User Account Management** en Office 365 le apoya durante la organización de los usuarios.
- **Microsoft Intune for Education** le ayuda a la hora de enumerar y gestionar una diversidad de dispositivos.
- **System Center** es una solución ideal para enumerar y gestionar servidores con varios OS y soluciones de hosting en la nube.
- **Azure Search** le ayuda a la hora de agregar funcionalidad de búsqueda avanzada en su entorno actual.
- **Azure Data Catalog** registra, descubre, entiende y consume fuentes de datos.
- **Cloud Discovery** analiza los registros de tráfico contra el catálogo de aplicaciones en la nube de Cloud App Security que incluye más de 15.000 aplicaciones en la nube que se clasifican y puntúan conforme a más de 60 factores de riesgo, ofreciéndole una visibilidad continua del uso en la nube, informática paralela y el riesgo que la informática paralela presenta para su organización.
- **Advanced Data Governance** (ADG) que le ayuda a identificar, clasificar y gestionar automáticamente datos personales y sensibles, además de aplicar políticas de retención y eliminación de los datos.

Gestionar

- Utilice **Security Groups** en Office 365 para establecer un conjunto de permisos único a través de todas las aplicaciones de Office 365.
- **Outlook smart attachments** previene que la información salga de la institución.
- **Utilice Office 365 mail tips** para evitar errores comunes.
- **Office 365 Data Loss Prevention** previene que la información salga del local.
- Crear **Flujos** automáticos entre aplicaciones optimizará y mantendrá seguros los flujos de datos.
- **Intune for Education** le ayuda a gestionar políticas, aplicaciones y configuraciones para los dispositivos utilizados en las aulas
- **Azure AD** (Azure Active Directory) es el directorio de Microsoft basado en la nube y el servicio de gestión de la identidad.
- Utilice **Power Apps** para crear aplicaciones móviles rápidamente e introducirlas directamente a la base de datos.
- Aplique **etiquetas** a los datos personales y gestione el **control de los datos** en Office 365.
- **Azure Information Protection**: Le ayudará a controlar y hacer seguros correos electrónicos, documentos y datos sensibles que comparte con otras fuentes ajenas a su empresa.
- Incrustar **Microsoft Forms** (Office 365) puede hacer segura la entrada de datos a través de formularios electrónicos y permitir el cumplimiento del RGPD durante las solicitudes de consentimiento.
- **Office 365 Teams** permite que las instituciones centralicen y coordinen todas las comunicaciones requeridas para las políticas del RGPD.

Informar

- **Microsoft Trust Center** es la fuente ideal para verificar la información sobre el RGPD y el cumplimiento.
- Microsoft **Compliance Manager** le ayuda a realizar evaluaciones de riesgos y simplifica sus procesos de cumplimiento, ofreciéndole acciones recomendadas, recopilación de evidencia y preparación para las auditorias.
- **Azure auditing and logging** le ofrece un registro electrónico de actividades sospechosas y le ayuda a detectar patrones que podrían indicar infiltraciones externas supuestas o de éxito de la red, además de ataques internos.
- **Securescore.office.com** es una herramienta analítica segura que le ayudará a entender lo que ha hecho para reducir el riesgo que corren sus datos en Office 365, además de indicarle otras medidas que podrá adoptar para reducir dicho riesgo. Es la fuente ideal de conocimientos de auditoria, registros y muchas otras funciones de seguridad de Office 365.
- **Unified audit log** le ofrece información de los datos que han sido transferidos a terceros.transferred to third parties.

Aviso: Esta no es una lista completa de las herramientas y servicios Microsoft disponibles para respaldar las cuatro etapas claves. Si desea una visión general más completa de cómo pueden ayudar a nuestros clientes los servicios y los productos Microsoft Cloud a cumplir sus obligaciones al amparo del RGPD, tenga la amabilidad de descargar el e-book titulado Microsoft Cloud agiliza el cumplimiento del RGPD

Proteger

- **Office 365 (A3) Data Loss Prevention** permite crear una serie de normas para prevenir que los tipos de información deseados salgan de la institución.
- **Azure Information Protection**: Le ayudará a controlar y hacer seguros correos electrónicos, documentos y datos sensibles que comparte con otras fuentes ajenas a su empresa. Desde la clasificación sencilla hasta etiquetas incrustadas y permisos, mejore siempre la protección de los datos con Azure Information Protection—independientemente de dónde se guarden o con quién se compartan.
- **Customer Lockbox**, puede habilitar que los controladores demuestren que tienen implantados procedimientos explícitos para acceder al contenido del cliente durante las operaciones de servicio.
- **AppLocker** ayuda a los administradores a crear y desplegar políticas de control para aplicaciones, limitando el acceso por parte de usuarios no autorizados a las aplicaciones que podrían presentar un riesgo para los datos personales.
- **Microsoft Advanced Threat Analytics (ATA)** es una plataforma instalada en la institución que ayuda a proteger su colegio de ciberataques avanzados múltiples y amenazas internas.
- **Office 365 Threat Intelligence.**
- **Intune for Education** es una solución sencilla pero robusta para poner en marcha políticas de seguridad, aplicaciones y configuraciones para los dispositivos que se utilizan en las aulas.
- **Windows Defender Advanced Threat Protection** disponible en Windows 10 Education es un servicio de seguridad que permite que los clientes empresariales detecten, investiguen y reaccionen ante amenazas avanzadas en sus redes.
- **Azure Backup** y **Azure Disaster Recovery** incrementan la disponibilidad.
- **BitLocker Drive Encryption** es una característica de protección que se integra en el sistema operativo y trata las amenazas de robo de datos o exposición procedente de los datos perdidos o robados o de ordenadores retirados de servicio de manera impropia.
- Utilice **Multi Factor Authentication** en Office 365 y Windows 10 con Windows Hello.Windows 10 with Windows Hello.

Este e-Book es un comentario sobre el RGPD, tal como Microsoft lo interpreta, en la fecha de publicación. Hemos dedicado mucho tiempo al estudio del RGPD y nos gustaría pensar que hemos sido considerados sobre su propósito y significado. Sin embargo, la aplicación del RGPD es muy hecho-específica, y no todos los aspectos e interpretaciones del RGPD están bien definidos.

Por ello, este e-book se ofrece a título informativo solamente y no debería confiarse en la información en él contenida como asesoramiento legal ni para determinar cómo el RGPD podría aplicarse a sus circunstancias personales y las de su organización. Le alentamos a que consulte a un profesional legal capacitado con el que discutir el RGPD, cómo se aplica específicamente a su organización y cómo mejor cumplir sus reglamentos.

MICROSOFT NO OFRECE GARANTÍAS, EXPRESAS, IMPLÍCITAS O ESTATUTARIAS SOBRE LA INFORMACIÓN CONTENIDA EN ESTE E-BOOK. Este e-book se proporciona "tal cual." La información y las opiniones expresadas en este e-book, incluyendo URL y otras referencias a páginas web en Internet, podría cambiar sin previo aviso.

Publicado en marzo de 2018 Versión 1.0