Los 6 mandamientos del GDPR

Cómo afecta el Reglamento General de Protección de Datos (GDPR) al marketing

Secciones

1. **Seguridad jurídica y práctica**
2. **Qué es, cuándo entra en vigor, a quién afecta**
3. **Los principios que rigen el GDPR**
4. **Guía de uso para el departamento de marketing**
5. **Test para saber si su organización cumple con el GDPR**
6. **El compromiso de Microsoft**
7. **¿Cómo ayudan las soluciones Microsoft al cumplimiento del GDPR?**
8. **Recursos y fuentes**

El GDPR amplía el control sobre los datos personales que compartimos y su utilización.

Sección 1

Seguridad jurídica y práctica

El avance de la integración económica y social de las entidades, empresas y organismos de los países miembros de la Unión Europea ha traído consigo un aumento de los flujos transfronterizos de los datos personales de sus ciudadanos. La transformación de las relaciones comerciales, la rápida evolución tecnológica y el aumento del volumen de intercambio de los datos que se produce actualmente entre personas físicas y empresas ha planteado un gran reto para la protección de los derechos ciudadanos.

Para dar cobertura legal a este tipo de transacciones y unificar la legislación existente, el Parlamento Europeo aprobó en abril de 2016 el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés).

> Las personas difunden un volumen cada vez mayor de información personal a escala mundial

Tal y como recoge dicho Reglamento, "la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades" y las personas difunden un volumen cada vez mayor de información personal a escala mundial.

Esta circunstancia, sin embargo, no debe colisionar con el derecho de los ciudadanos a tener el control sobre sus propios datos personales.

El GDPR viene, por tanto, a reforzar la seguridad jurídica y práctica de este tipo de transacciones para que tanto las personas como los operadores económicos y las autoridades públicas estén amparadas bajo una norma global.

Sección 2

Qué es, cuándo entra en vigor, a quién afecta

¿Qué es el GDPR?

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) es la nueva normativa europea de privacidad.

¿Cuándo entra en vigor?

Entró en vigor en mayo de 2016 tras su aprobación en el Parlamento Europeo, aunque su aplicación obligatoria se iniciará en mayo de 2018.

¿Qué ocurre con las normas existentes en cada país miembro de la UE?

Las normas de protección de datos aprobadas por los estados miembros de la Unión Europea quedarán relegadas por la aplicación del nuevo GDPR, que será de aplicación directa sin que ningún país tenga que desarrollar ni modificar sus leyes anteriores. En el caso de España, hasta el momento la normativa aplicable era la recogida en la Ley Orgánica de Protección de Datos (LOPD), que se verá así superada por el nuevo reglamento europeo.

¿A quién afecta?

A instituciones públicas, organizaciones sin ánimo de lucro y todo tipo de empresas que recopilan y analizan datos de ciudadanos residentes en la Unión Europea (UE).

Ahora bien, el Reglamento incluye excepciones para las microempresas, las pequeñas y medianas empresas y las organizaciones con menos de 250 empleados. En concreto, estas empresas no estarán obligadas a tener un registro de las actividades del tratamiento de los datos que atesoran.

¿El GDPR se aplica también a las empresas radicadas fuera de la UE?

Sí. El GDPR se aplica a todas las compañías que realicen tratamiento de datos de ciudadanos de la Unión, bien porque les ofrezcan sus bienes o servicios o bien como consecuencia de acciones de monitorización y seguimiento de su comportamiento.

¿Qué tipo de sanciones conllevará su incumplimiento?

Las organizaciones pueden enfrentarse a multas de hasta 20 millones de euros o el 4% de su volumen de negocio global anual.

¿Qué se consideran 'datos personales'?

'Datos personales' es cualquier información relacionada con una persona identificada o identificable. No hay distinción entre las funciones privadas, públicas o laborales de una persona.

Los datos personales pueden incluir:

- ✓ **Nombre**
- ✓ **Domicilio**
- ✓ **Dirección del trabajo**
- ✓ **Número de teléfono**
- ✓ **Dirección de correo electrónico**
- ✓ **DNI o equivalente**
- ✓ **Información física, fisiológica o genética**
- ✓ **Información médica**
- ✓ **Identidad cultural**
- ✓ **Número de cuenta bancaria**
- ✓ **Número de tarjeta de crédito / débito**
- ✓ **Perfiles de redes sociales**
- ✓ **Publicaciones en redes sociales**
- ✓ **Dirección IP**
- ✓ **Ubicación / datos de GPS**
- ✓ **Cookies**

¿El GDPR afecta a todas las empresas que trabajan con datos personales o únicamente a las propietarias de los mismos?

A todas. Si en tu caso trabajas con los datos personales que te facilitan tus clientes o socios también debes tener en cuenta los requisitos que marca el GDPR, que afecta por igual a los denominados "controladores" o dueños de los datos que a los "procesadores" que trabajan sobre los mismos en nombre del controlador.

Sección 3

Los principios básicos que rigen el GDPR

El principal objetivo del GDPR es otorgar a los residentes de la UE un mayor control sobre sus datos personales, ampliando las obligaciones que deben cumplir las organizaciones.

Según el propio Reglamento, "la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental". Como tal está recogido en la Carta de los Derechos Fundamentales de la Unión Europea y en el Tratado de Funcionamiento de la Unión Europea (TFUE).

La protección de los datos personales es un derecho fundamental

Los principales preceptos que establece el Reglamento europeo son:

1. Transparencia. Las organizaciones deben informar a los ciudadanos sobre la licitud de la captación y uso de sus datos personales.

2. Consentimiento claro y expreso. Las empresas sólo pueden utilizar los datos para los fines específicos para los que fueron recopilados.

3. Minimizar la recopilación. La captación de datos indiscriminada no estará permitida. Las organizaciones podrán recoger sólo aquellos datos pertinentes para el fin previsto.

4. Exactitud de la información, derecho al olvido y portabilidad. Los ciudadanos podrán exigir la modificación, borrado o traspaso a terceros de sus datos personales contenidos en los ficheros de las compañías.

5. Almacenamiento limitado. Los datos personales sólo podrán ser almacenados por el tiempo necesario para lograr los fines para los que fueron recogidos.

6. Garantía de seguridad. Las organizaciones deben garantizar la seguridad y confidencialidad de los datos personales almacenados.

Tres elementos de carácter general constituyen la mayor innovación del GDPR:

1. El principio de responsabilidad proactiva

¿Qué es?

Hace referencia a la obligación de las organizaciones de garantizar técnicamente el cumplimiento del GDPR. Engloba varias medidas que toda entidad debe tener en cuenta y que sirven como hoja de ruta para el **diseño de un proceso estándar de tratamiento de datos**:

- ✓ **Protección de datos desde el diseño**
- ✓ **Protección de datos por defecto**
- ✓ **Medidas de seguridad**
- ✓ **Mantenimiento de un registro de tratamientos**
- ✓ **Realización de evaluaciones de impacto sobre la protección de datos**
- ✓ **Nombramiento de un delegado de protección de datos**
- ✓ **Notificación de violaciones de la seguridad de los datos**
- ✓ **Promoción de códigos de conducta y esquemas de certificación**

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.

Y, en función de esa información, deberán establecer los protocolos a seguir en cada caso.

2. El enfoque de riesgo

¿Qué es?

Se refiere a que la aplicación de las medidas previstas por el GDPR deben adaptarse a las características de las organizaciones y el tipo de datos que tratan. No tendrá que cumplir con las mismas obligaciones una compañía que recaba datos de carácter sanitario, o volúmenes de datos de millones de interesados, que una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

3. El responsable de datos

¿Es obligatorio tener un "responsable de datos"?

Sí. Todas las organizaciones deberán nombrar un representante que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos. Los datos de contacto de ese representante deberán proporcionarse a los interesados.

Además, el Reglamento recoge que los responsables de datos:

- ✓ **Deben mantener un registro de actividades de tratamiento.**
- ✓ **Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.**

El departamento de marketing deberá exigir al responsable de los datos que lleve a cabo una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

El tipo de análisis variará en función de:

- **los tipos de tratamiento**
- **la naturaleza de los datos**
- **el número de interesados afectados**
- **la cantidad y variedad de tratamientos que una misma organización lleve a cabo.**

Sección 4

Guía de uso para el departamento de marketing

La aplicación del GDPR afecta de forma directa al desarrollo de la actividad de los departamentos de Marketing. Sin embargo, aunque el texto legal aprobado por el Parlamento Europeo es exigente, **la normativa nacional vigente hasta el momento ya recogía el espíritu y los preceptos básicos del nuevo reglamento**.

Este hecho conlleva que la aplicación del mismo no tenga por qué suponer ningún problema para los departamentos de marketing que, eso sí, deben conocer los principales cambios y exigencias que marca el GDPR en cuanto a las comunicaciones comerciales y el tratamiento de los datos.

> La aplicación del GDPR no debe suponer ninguna complicación para el equipo de marketing.

En las siguientes páginas vamos a exponer y ejemplificar las principales cuestiones y tareas que lleva a cabo un equipo de marketing y que se verán afectadas por la aplicación del GDPR.

Transparencia

Las organizaciones deben informar a los ciudadanos sobre la licitud de la captación y uso de sus datos personales.

Por ejemplo, cuando el departamento de marketing recaba datos personales a través de un formulario ubicado en la página web, debe ofrecer a los usuarios la siguiente información:

- ✓ **La base legal sobre la que se desarrolla el tratamiento -una referencia a la norma que ampara dicha captación de datos, pero sin utilizar un lenguaje farragoso.**
- ✓ **Especificación sobre el uso de los datos. Por ejemplo, explicando que el uso será de carácter informativo y comercial.**

La Agencia Española de Protección de Datos (AEPD) recomienda incluir la siguiente información en los documentos o soportes electrónicos utilizados para recabar datos personales:

- ✓ **Base jurídica del tratamiento**
- ✓ **Intención de realizar transferencias internacionales (si la hubiere)**
- ✓ **Datos del Delegado de Protección de Datos**
- ✓ **Referencia al uso de los datos para la elaboración de perfiles si fuera el caso**

El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea **fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.**

Las organizaciones deben ser capaces de demostrar que el usuario ha otorgado su consentimiento, y para ello necesitará usar sistemas técnicos verificables.

¿Cómo debe ser un aviso de privacidad?

El GDPR obliga a las entidades a informar en sus avisos de privacidad de:

- ✓ **la base legal que da cobertura al tratamiento de los datos**
- ✓ **el período de retención de los mismos**
- ✓ **y los pasos que deben seguir los interesados para realizar cualquier reclamación.**

La norma exige de forma expresa que la información que se proporcione sea fácil de entender y que se presente en un lenguaje claro y conciso.

Uso en mercadotecnia

Tal y como establece el Reglamento, "si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener **derecho a oponerse a dicho tratamiento**, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello **en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente** al interesado y presentarse claramente y al margen de cualquier otra información".

Consentimiento claro y expreso

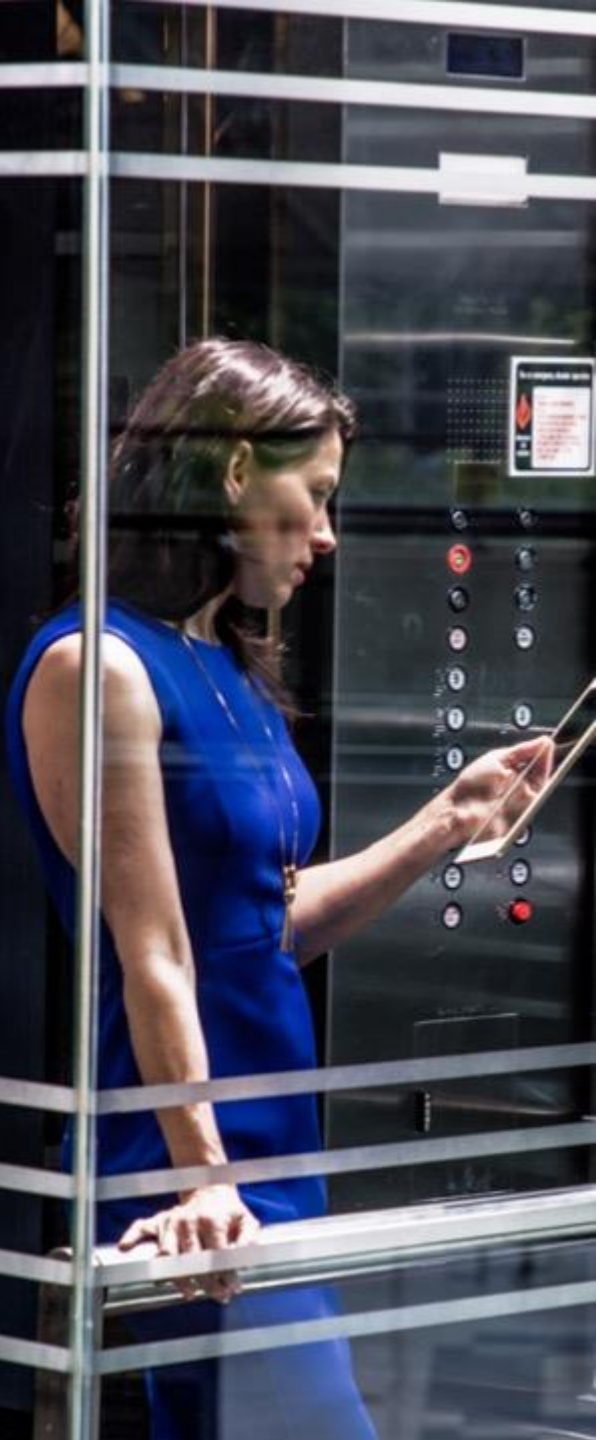
Las empresas sólo pueden utilizar los datos para los fines específicos para los que fueron recopilados.

Esto podría incluir marcar una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de **voluntad libre, específica, informada e inequívoca** del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.



el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

Por ejemplo, si los datos recabados en un formulario web o acción de marketing se van a usar para la participación de un usuario en un concurso, pero también se hará uso de ellos posteriormente para el envío de ofertas comerciales y, además, se utilizarán para realizar un estudio sobre el perfil de los consumidores de la marca, la empresa debe explicar de forma sencilla y clara cada uno de esos usos, y el usuario tendrá que dar su consentimiento explícito a los mismos.

El denominado "consentimiento tácito" dejará de ser legal.

Cuando se trate de **datos "sensibles"** -como los referentes a la salud- no será suficiente con una acción positiva de carácter general, sino que deberá especificarse explícitamente el tipo de tratamiento de los datos que se realizará.

¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?

Según recoge el GDPR, "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

El Reglamento europeo establece como edad límite inferior los 13 años, pero la normativa española fija ese tope en los 14 años. Por debajo de esa edad es necesario el consentimiento de padres o tutores.

Minimizar la recopilación

La captación de datos indiscriminada no estará permitida. Las organizaciones podrán recoger sólo aquellos datos pertinentes para el fin previsto.

El responsable de datos de cada compañía debe llevar un "Registro de las actividades de tratamiento".

Dicho registro deberá contener toda la información indicada a continuación:

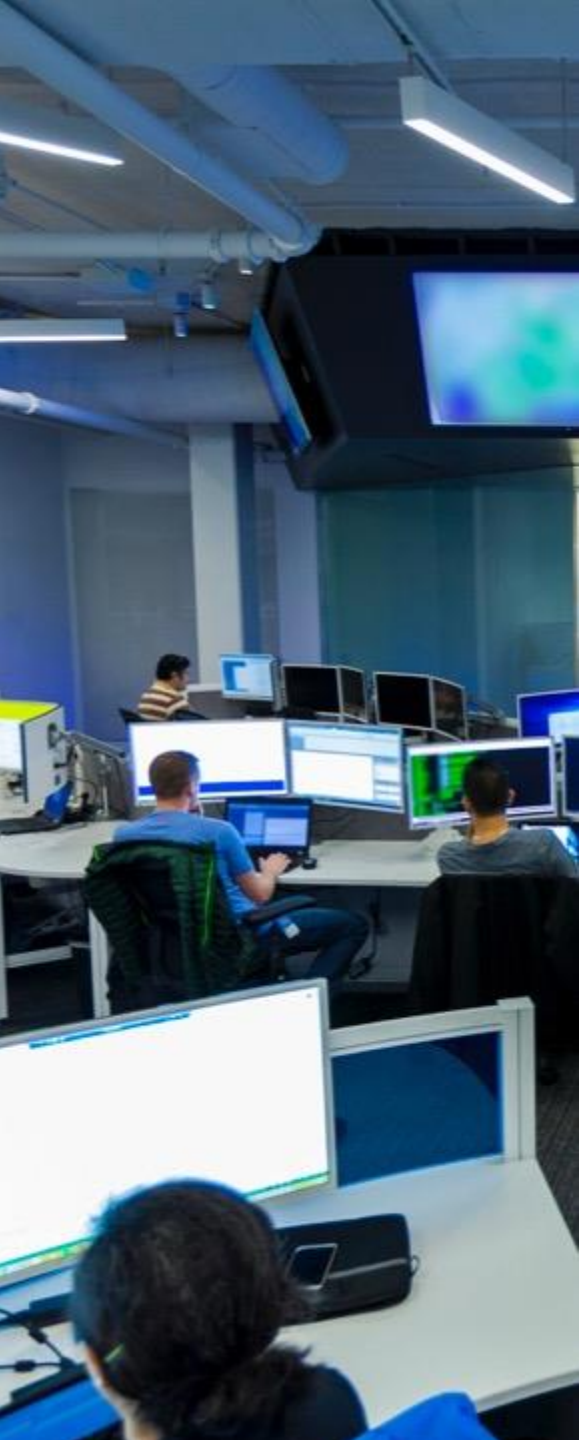
- ✓ **El nombre y los datos de contacto del responsable**
- ✓ **Los fines del tratamiento**
- ✓ **Una descripción de las categorías de interesados y de las categorías de datos personales**
- ✓ **Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales**
- ✓ **En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional**
- ✓ **Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos**
- ✓ **Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad referentes a la salvaguarda de esos datos**

Exactitud de la información, derecho al olvido y portabilidad

Los ciudadanos podrán exigir la modificación, borrado o traspaso a terceros de sus datos personales contenidos en los ficheros de las compañías.

Las organizaciones que trabajan con datos personales deberán:

- ✓ **Definir los procesos para facilitar al interesado el ejercicio de sus derechos de forma gratuita.**
- ✓ **Proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos.**
- ✓ **Informar al interesado sobre las actuaciones derivadas de su petición**



en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación).

¿Qué es el derecho al olvido?

Es el derecho que tienen los ciudadanos a solicitar que sus datos personales sean suprimidos de una base de datos, se bloqueen de las listas de resultados de los buscadores, etcétera.

Es una **manifestación de los derechos de cancelación u oposición en el entorno online** (según la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain).

Las compañías que actualmente se ajustan a la jurisprudencia existente en relación al derecho al olvido no tienen que modificar sus prácticas.

¿Qué es el derecho a la portabilidad?

Se refiere al derecho que tiene un ciudadano de solicitar una copia de sus datos a una compañía.

El GDPR establece como novedad que la copia que se proporcione al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica.

Este derecho sólo puede ejercerse:

- **Cuando el tratamiento se efectúe por medios automatizados.**
- **Cuando el tratamiento se base en el consentimiento o en un contrato.**
- **Cuando el interesado lo solicite respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.**

Almacenamiento limitado

Los datos personales sólo podrán ser almacenados por el tiempo necesario para lograr los fines para los que fueron recogidos.

En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados.

Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación.

La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Garantía de seguridad

Las organizaciones deben garantizar la seguridad y confidencialidad de los datos personales almacenados.

El GDPR se refiere a las violaciones de seguridad de los datos o "quiebras de seguridad" como **todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos**.

Por ejemplo, sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del GDPR.

Si eso ocurre, el responsable de los datos deberá notificar dicha circunstancia a la autoridad competente dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Además, llegado el caso también sería necesario informar de dicha quiebra de seguridad a las personas cuyos datos están en riesgo.

Los productos y servicios de Microsoft, como Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 y Windows 10 garantizan la detección y evaluación de amenazas de seguridad y el cumplimiento de las obligaciones del GDPR.

Sección 5

Test para saber si su organización cumple con el GDPR

Conteste a las siguientes cuestiones que le planteamos para conocer el grado de cumplimiento del GDPR de su departamento de Marketing u organización. Esta reflexión le ayudará a valorar si necesita reforzar sus protocolos, modificar sus métodos de trabajo o solicitar ayuda a un equipo externo.

- ✓ **¿Sabe cuál es la base legal de los tratamientos que realiza?**
- ✓ **Sus solicitudes de consentimiento en la web, landing pages, folletos, etcétera, ¿reúnen los requisitos que exige el GDPR?**
- ✓ **La información que proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?**
- ✓ **¿Contiene esa información todos los elementos que prevé el GDPR?**
- ✓ **¿Dispone de mecanismos para el ejercicio de los derechos de olvido, rectificación o portabilidad de los datos personales de los usuarios?**
- ✓ **¿Conoce las medidas de seguridad que se aplican a los datos que recoge en sus acciones de marketing?**
- ✓ **¿Cuenta con la tecnología necesaria para identificar con rapidez la existencia de violaciones de seguridad de los datos?**

Sección 6

El compromiso de Microsoft

La nube de Microsoft está específicamente diseñada para ayudarle a centralizar y simplificar los pasos técnicos y administrativos, comprender los riesgos y defenderse de ellos, y con frecuencia es más segura que los tradicionales entornos informáticos locales. Nuestra amplia red de expertos y la total coordinación con nuestros partners hacen de los productos de Microsoft la mejor solución en áreas clave de su negocio, como es la seguridad de los datos, los dispositivos y las infraestructuras.

Cumplir el Reglamento General de Protección de Datos (GDPR) no es una opción, es una obligación que usted puede convertir en una oportunidad de negocio.

Sección 7

¿Cómo ayudan las soluciones Microsoft al cumplimiento del GDPR?

Detectar

Encuentre y clasifique datos fácilmente con:

- **Azure Data Catalog, un servicio en la nube que permite detectar el origen de los datos.**
- **Office 365 Advanced eDiscovery para encontrar texto y metadatos de Exchange, SharePoint, Skype, Onedrive, etc.**
- **Cloud App Security de Enterprise Mobility + Security, que le permitirá evaluar riesgos y detectar amenazas.**
- **Windows Search para rastrear y localizar datos en máquinas locales y en cualquier dispositivo conectado al que tenga los permisos para acceder.**

Gestionar

Gestione sus políticas de gobernanza de datos con:

- **Journaling (Exchange Online) de Office 365 para registrar sus comunicaciones.**
- **Azure Active Directory (Azure AD) para garantizar que sólo los usuarios autorizados tengan acceso a los entornos informáticos, los datos y las aplicaciones.**
- **Azure Information Protection para clasificar y proteger la información confidencial que comparte.**
- **Microsoft Intune para controlar el acceso, cifrar dispositivos, eliminar datos de dispositivos móviles de forma selectiva y controlar qué aplicaciones almacenan y comparten datos.**

Proteger

Proteja el correo electrónico y los datos almacenados en ordenadores, servidores y dispositivos con:

- **Advanced Threat Protection de Office 365 para protegerse contra los archivos adjuntos no seguros o vínculos malintencionados.**
- **Utilice Microsoft Intune de Enterprise Mobility + Security para que sus empleados trabajen en dispositivos móviles sin poner en riesgo la información de su empresa.**
- **Windows Defender ATP para detectar, investigar e informar de filtraciones.**
- **Azure Advanced de Enterprise Mobility + Security.**

Informar

Evalúe los riesgos con herramientas integradas y haga un seguimiento e informes de actividad detallados con:

- **Service Assurance Dashboard de Office 365**
- **Windows Defender**
- **Customer Lockbox de Office 365 para otorgar autorización expresa de acceso a los datos durante las operaciones de servicio.**
- **Azure AD Advanced Reports para ayudar en la respuesta a posibles amenazas y recibir análisis sobre acceso a dispositivos y el uso de aplicaciones.**

Sección 8

Recursos y fuentes

Herramienta de Evaluación de GDPR

Centro de Confianza

Microsoft para las Empresas

Proveedores de soluciones Microsoft

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Guía del Reglamento General de Protección de Datos para responsables de tratamiento elaborado por la Agencia Española de Protección de Datos.

Microsoft

Contacto
Plaza Roma
F1, 1ª planta
50010 Zaragoza
976 46 76 76
marketing@efor.es
www.efor.es

Sobre EFOR

EFOR es una compañía tecnológica Gold Partner de Microsoft especializada en desarrollo de software, marketing digital, soluciones tecnológicas, sistemas y formación técnica.

TE AYUDAMOS EN LA ADAPTACIÓN AL GDPR

Desde EFOR garantizamos el éxito en tu proceso de adaptación, poniendo a tu alcance soluciones para cada área de actuación del **GDPR.**

1. **Análisis de situación:** auditoría y diagnóstico.
2. **Cumplimiento normativo**: ProQuo GDPR Compliance
3. **Aplicación de medidas técnicas**: tras la evaluación de riesgos

Más información sobre nuestros servicios en **www.efor.es/gdpr**