Reglamento General de Protección de Datos de la UE

Una guía de cumplimiento

Diciembre de 2016

Proteger • Cumplir • Progresar

Prepararse para el cumplimiento del RGPD

El Reglamento General de Protección de Datos (RGPD) supone el cambio más significativo de la ley de protección de datos a nivel europeo y mundial de los últimos 20 años. En este libro verde, ofrecemos una visión completa de los cambios claves introducidos por el Reglamento y de las áreas críticas a tener en cuenta para su cumplimiento.

Introducción

El Reglamento General de Protección de Datos (RGPD) de la UE se adoptó en abril de 2016 y será de aplicación directa en toda la Unión Europea (UE) el 25 de mayo de 2018, cuando sustituya las 28 leyes de protección de datos nacionales que se basan en la Directiva de Protección de Datos (DPD) de 1995.

Introducido para seguir los avances del panorama digital moderno, el RGPD tiene un doble propósito:

1. Mejorar la confianza del consumidor en las organizaciones que guardan y procesan sus datos personales, reforzando así sus derechos de privacidad y seguridad.
2. Simplificar el libre flujo de datos personales en la UE mediante un marco sistemático y coherente de protección de datos en todos los Estados miembros.

El nuevo Reglamento no cambia fundamentalmente ninguna norma principal de la DPD; en su lugar amplia los requisitos de la Directiva considerablemente al introducir una variedad de nuevas obligaciones para apoyar estas normas principales. Estas obligaciones adicionales serán familiares en algunos Estados miembros. Por ejemplo, Alemania ya impone una obligación de nombrar delegados de protección de datos, tiene el concepto de datos seudonimizados y tiene requisitos exhaustivos para los contratos de procesadores. Sin embargo, estas obligaciones serán muy nuevas para otros países.

Un asunto de urgencia

Cada organización que procese o comparta datos personales tiene hasta el 25 de mayo de 2018 para cumplir el nuevo Reglamento. Esto implica que las organizaciones tienen que saber qué datos personales guardan o procesan actualmente y los riesgos de esos datos. Además, se tienen que adaptar los procesos y la estructura empresarial, así como implementar herramientas y procesos de cumplimiento que actualicen la manera de colaborar con los proveedores. En algunos casos, estos cambios podrían ser importantes y tendrán que empezar a trabajar como asunto de urgencia.

El cumplimiento reglamentario puede ser visto por muchos como una carga administrativa. Sin embargo, ignorar el RGPD o no cumplirlo en su totalidad puede conllevar **multas administrativas de hasta el 4 % de la facturación global anual global del ejercicio anterior o 20 millones de euros**, lo que sea mayor.

Las organizaciones que dediquen tiempo a prepararse adecuadamente y cumplir el nuevo Reglamento no solo evitarán estas multas importantes, sino también la pérdida de su reputación empresarial. Además, conseguirán el tratamiento de sus datos, la información de seguridad, los procesos de cumplimiento y las relaciones contractuales sean más sólidos y fiables.

Cambios clave:

GLOSARIO

Responsable de los datos (organización): persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de los datos personales.

Interesado (persona): persona física identificable con toda persona "cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización o un identificador en línea".

Datos personales: toda información sobre una persona física identificada o identificable ("el interesado")". El Reglamento indica que esto también incluye los identificadores en línea tales como las direcciones IP y las cookies.

Encargado del tratamiento (prestadores del servicio): persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Un ejemplo es un proveedor en la nube que ofrece almacenamiento de datos.

1. Ámbito de la nueva ley

Armonización, solo una ley

Actualmente, hay 28 grupos diferentes de leyes de protección de datos en toda la Unión Europea. El RGPD las reemplazará adoptando un marco reglamentario paneuropeo desde el 25 de mayo de 2018. Como Reglamento, tendrá vigor directamente en todos los estados miembros sin la necesidad de legislación nacional adicional.

Para las organizaciones que operan en múltiples Estados miembros, esta armonización es bien recibida. Sin embargo, es probable que se mantengan algunas divergencias nacionales y más divergencias pueden surgir porque los países tienen derechos limitados para modificar algunas de las obligaciones según el Reglamento:

- Empleo: los estados miembros pueden introducir más restricciones en el tratamiento de los datos de los empleados.
- Seguridad nacional: los estados miembros pueden aprobar una ley para limitar los derechos según el Reglamento en áreas tales como la seguridad nacional, delitos y los procedimientos judiciales.

Aunque el Reglamento ha sido publicado, hay todavía incertidumbre acerca de lo que significan algunas de las disposiciones o cómo se deben aplicar. Las distintas actitudes sociales y culturales con la protección de datos influirán en su interpretación y lo que se considera "alto riesgo" en Berlín puede que no sea considerado como tal en Roma.

Finalmente, las diferencias en los recursos y las actitudes de las autoridades de control pueden dar como resultado amplias variaciones en la aplicación. Hay una gran discrepancia entre las facultades teóricas abiertas a las autoridades de control nacionales y la aplicación de esas facultades en la práctica.

Cuestiones de este tipo se resolverán en el transcurso normal del asunto reglamentario. Las organizaciones todavía afrontan la fecha límite del cumplimiento del 25 de mayo de 2018.

Alcance territorial ampliado

El RGPD se aplica a todas las organizaciones de la UE, ya sean empresas comerciales o autoridad pública, siempre y cuando recopilen, almacenen o traten datos personales de residentes europeos.

Las organizaciones con sede fuera de la UE que monitoricen u ofrezcan productos y servicios a personas en la UE tendrán que seguir las nuevas normas europeas y acatar el mismo nivel de protección de datos personales.

El Reglamento también exige que dichas organizaciones, responsables y encargados del tratamiento, nombren un representante en la UE con sede en uno de los estados miembros en los que estén radicadas las personas pertinentes. Esto es a menos que el tratamiento sea ocasional y no incluya el tratamiento a larga escala de categorías especiales de datos o el tratamiento de datos relativos a condenas y delitos penales.

Un solo sistema 'integral'

Una nueva disposición integral significa que las organizaciones solo tendrán que tratar con una sola autoridad de control, no una para cada uno de los 28 estados miembros de la UE, haciendo que esto sea más sencillo y barato para hacer negocios en la UE. Una organización que realice un tratamiento transfronterizo debe estar regulada principalmente por la autoridad de control donde tenga su

establecimiento principal (la autoridad de control principal).

Obligaciones en los encargados

El Reglamento también introduce obligaciones para los encargados del tratamiento de los datos. Estos son prestadores de servicios que tratan datos personales en nombre de empresas, pero no determinan el propósito ni medios del tratamiento, tales como los servicios telefónicos de atención al cliente.

Cuando un responsable del tratamiento contrate un encargado para el tratamiento de los datos personales, ese encargado debe ser capaz de ofrecer "garantías suficientes para aplicar medidas técnicas y organizativas apropiadas", asegurando así el cumplimiento del RGPD y que se protegen los derechos de los interesados. Este requisito desciende por la cadena de suministro, por tanto, un encargado no puede subcontratar trabajo a un segundo encargado sin la autorización explícita del responsable.

Los acuerdos contractuales tendrán que actualizarse y será imperativo estipular las responsabilidades y obligaciones entre el responsable y el encargado en los futuros acuerdos. Las partes tendrán que documentar sus responsabilidades de datos incluso de forma más clara. Asimismo, el aumento de los niveles de riesgo puede tener un impacto en los costes del servicio.

2. Derechos de datos de las personas

Las normas principales se mantienen

Muchas de las definiciones principales de la DPD no se verán alteradas. En particular, el Reglamento mantiene una definición muy amplia de datos personales y tratamiento, y las organizaciones deben cumplir todos los principios generales cuando traten los datos personales. Algunos conceptos nuevos son "personas de alto riesgo", "tratamiento a gran escala" y "datos pseudonimizados" (datos con los cuales ninguna persona se puede identificar sin el uso de información adicional).

Consentimiento

El Reglamento impone requisitos más estrictos para obtener el consentimiento válido de las personas para justificar el tratamiento de sus datos personales. El consentimiento debe ser una "manifestación de voluntad libre, específica, informada e inequívoca del interesado". El silencio, casillas premarcadas o la inactividad no cuentan como consentimiento. La organización debe conservar también registros para que pueda demostrar que el consentimiento ha sido dado por la persona pertinente. Finalmente, el consentimiento debe ser explícito cuando se traten datos personales sensibles o se transfieran datos personales fuera de la UE.

Protección adicional para menores

El consentimiento de un menor en relación con los servicios en línea, según el nuevo Reglamento solo es válido si está autorizado por uno de los padres. Un menor es alguien menor de 16 años, aunque los estados miembros pueden reducir esta edad a 13.

Nuevo derecho de acceso a los datos

Uno de los objetivos clave del Reglamento es facultar a las personas y darles el control sobre sus datos personales. Aunque el Reglamento conserva en gran medida los derechos existentes de las personas para acceder a sus propios datos personales, exigir la corrección de datos inexactos, objetar al marketing directo y desafiar las decisiones automáticas sobre ellos, también confiere importantes nuevos derechos adicionales para las personas.

- **Derecho al olvido**
  Los interesados tienen derecho a exigir al responsable del tratamiento que se suprima cualquier dato personal que se conserve de estos bajo una serie de circunstancias como, por ejemplo, cuando los datos ya no son necesarios para los fines para los cuales fueron recopilados. Hay una serie de excepciones a este derecho con relación a la libertad de expresión y al cumplimiento de las obligaciones legales. Es probable que los límites de este derecho se peleen en los tribunales de derecho de la UE durante muchos años.

- **Derecho a la portabilidad de los datos**
  Este es un nuevo concepto según el Reglamento. Las personas tendrán el derecho a transferir los datos personales de un responsable del tratamiento a otro cuando el tratamiento se base en el consentimiento o la

necesidad para el cumplimiento del contrato o cuando el tratamiento se lleve a cabo por medios automáticos.

Elaboración de perfiles

Los responsables del tratamiento deben informar a los interesados de la existencia y consecuencias de cualquier actividad de elaboración de perfiles que lleven a cabo (incluido el seguimiento en línea y la publicidad conductual).

Las organizaciones que recopilen y usen datos personales tendrán que implantar avisos de privacidad más severos de lo que se exigió anteriormente, facilitando más información de una manera más prescrita. Esto implicará una revisión a gran escala de todos los avisos de privacidad.

3. Protección de datos

Protección de datos desde el diseño

El Reglamento no se puede satisfacer con el cumplimiento de "casillas para marcar"; el cumplimiento debe convertirse en parte de "la actividad empresarial cotidiana". La clave de la responsabilidad es integrar el cumplimiento en la estructura de su organización. Esto incluye no solo desarrollar políticas adecuadas, sino también aplicar los principios de **la protección de datos desde el diseño y por defecto.**

Concretamente, las organizaciones deben tomar medidas técnicas y organizativas adecuadas antes de que empiece el tratamiento de datos para asegurarse de que cumple los requisitos del Reglamento. Los riesgos de la privacidad de datos deben evaluarse adecuadamente, y los responsables pueden utilizar la observancia de códigos conducta aprobados o certificaciones de sistemas de gestión, tales como la norma ISO 27001, para demostrar su cumplimiento.

Evaluación de Impacto relativa a la Protección de Datos (EIPD por sus siglas en inglés)

La protección de datos ahora debe diseñarse en sistemas de tratamiento por defecto y una evaluación de impacto relativa a la protección de datos será obligatoria bajo determinadas circunstancias. Hay que evaluar la buena práctica de las nuevas tecnologías y procesos si el tratamiento tiene un "alto riesgo" de perjudicar los derechos de los "interesados" y si el riesgo se puede reducir o evitar, por ejemplo, con pseudonimización. Una evaluación de impacto relativa a la protección de datos "en particular" puede ser necesaria cuando hay un tratamiento automático (incluido el archivo) y el tratamiento de categorías especiales de datos a gran escala.

Normas de cumplimiento

El RGPD fomenta la adopción de programas de certificación como medio de demostrar el cumplimiento. El cumplimiento de la norma internacional de seguridad de información ISO 27001, la única norma de seguridad de los datos reconocida internacionalmente, ayudará a las organizaciones a demostrar que se han esforzado en cumplir los requisitos de la seguridad de los datos del RGPD. Implementar ISO 27001 implica establecer un marco holístico de procesos, personas y tecnologías con el fin de asegurar la información.

Registros de tratamiento de los datos

El Reglamento ahora coloca la responsabilidad en las organizaciones y los responsables del tratamiento de mantener sus propios registros de actividades de tratamiento de los datos y poner estos a disposición de la autoridad de control. Este registro tiene que contener un conjunto específico de información para que sea claro el dato que se está tratando, dónde se está tratando, cómo se está tratando y por qué se está tratando. Las empresas pequeñas que empleen menos de 250 empleados están exentas de estos requisitos de conservación de registros a menos que sus actividades de tratamiento impliquen un riesgo para los derechos y libertades de los interesados, no sean ocasionales o incluyan categorías especiales de datos personales o datos relativos a condenas o delitos penales.

4. Responsabilidad

Delegado de Protección de Datos

A muchas organizaciones se les pedirá que nombren un Delegado de Protección de Datos (DPD O DPO por sus siglas en inglés) para que sea responsable de supervisar el cumplimiento del Reglamento, proporcionar información y asesoramiento y trabajar en colaboración con la autoridad de control. Son una característica existente de algunas leyes de protección de datos de los estados miembros, como Alemania.

Un delegado de la protección de datos debe nombrarse cuando:

- El tratamiento se lleva a cabo por una autoridad pública;
- Las actividades principales de la organización requieran una observación habitual y sistemática de los interesados a gran escala; o
- Las actividades principales de la organización consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

En la mayoría de las organizaciones sería recomendable nombrar un delegado de la protección de datos. Las obligaciones del RGPD son tan extensas que tener la orientación y apoyo de un especialista en protección de datos será una medida esencial en la gestión del riesgo, así como ya sucede cuando se nombra un gerente de RR. PP., salud y seguridad.

El delegado de la protección de datos, cuando sea nombrado, debe ser independiente. Esto no significa que tiene que nombrar una persona externa; la función del delegado de la protección de datos puede ser desempeñada por un empleado. El puesto puede ser una función a tiempo parcial o combinada con otros deberes, pero, al desempeñar la función, el delegado de la protección de datos debe tener una vía jerárquica independiente y debe estar facultado para informar directamente al consejo sin interferencias. Lo que es importante es que la persona nombrada debe ser un profesional en protección de datos con "conocimiento especializado de la ley y prácticas de protección de datos" para desempeñar sus funciones.

- **¿Qué cualificación necesita el delegado de la protección de datos?**

  El delegado de la protección de datos debe tener las cualidades profesionales adecuadas y conocimiento de la ley de protección de datos. En la actualidad no hay un requisito expreso de tener ninguna cualificación o certificado en concreto. Sin embargo, obtener formación y cualificaciones en cumplimiento del RGPD sería una manera eficaz de demostrar conocimiento especializado. El profesional del RGPD UE certificado con IBITGQ ISO 17024 es una de dichas cualificaciones.

Notificación de la violación de datos y sanciones

El aumento de los ciberataques de perfil alto se refleja en las obligaciones de una mayor seguridad de datos en el Reglamento y en las obligaciones paralelas en la **Directiva sobre la Seguridad de las Redes y Sistemas de Información.**

Será obligatorio que una organización denuncie cualquier violación de los datos a su autoridad de control en el plazo de 72 horas desde que tuvo conocimiento de esta. Si este requisito no se cumple, el informe final debe ir acompañado de una explicación detallada sobre el retraso. La notificación debe incluir información específica, la cual incluye una descripción de las medidas tomadas para abordar la violación y mitigar sus posibles efectos secundarios.

Cuando la violación puede ocasionar un alto riesgo para los derechos y libertades de las personas, hay que ponerse en contacto con ellas "sin dilación indebida". Este contacto no será necesario si hay implantadas medidas de protección apropiadas, fundamentalmente el cifrado, para eliminar el peligro para los interesados.

Cualquier infracción del nuevo Reglamento está sujeta a un régimen graduado de sanciones económicas con **multas hasta un 4 % de la facturación global anual del ejercicio anterior o 20 millones de euros, la que sea mayor**. Al determinar el nivel de la multa, la autoridad de control debe considerar una variedad de factores que incluyen la gravedad de la violación, si esta fue intencionada o el resultado de negligencia y cualquier medida tomada para mitigar la violación. Además, las personas pueden demandar a las organizaciones para conseguir una indemnización para cubrir tanto los daños materiales con los no materiales (p. ej. angustia).

Dada la magnitud de las multas potenciales, los derechos de las personas para ir a juicio y exigir indemnización, y el predominio y la eficacia del ciberdelito, un riesgo de violación de los datos debería ir directamente al registro de riesgo del consejo, y con cumplimiento alto en la prioridad de la alta dirección.

5. Transferencias de datos fuera de la UE

El Reglamento prohíbe la transferencia de datos personales fuera de la UE a un país tercero que no tenga una protección de datos adecuada. La Comisión Europea tiene el poder de aprobar países concretos como que proporcionan un nivel adecuado de protección de datos, teniendo en consideración las leyes de protección de datos en vigor en ese país y sus compromisos internacionales. En la actualidad esta lista es Andorra, Argentina, Canadá, Islas Faroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza y Uruguay.

Para las transferencias de datos a cualquier país que no esté en la lista, debe haber un contrato legal que estipule que el destinatario que no es de la UE acepta las garantías de protección de los datos exigidas. El Reglamento reconoce explícitamente y fomenta el uso de normas corporativas vinculantes como mecanismo de transferencia de datos válido en los grupos de empresas. Los códigos de conducta aprobados también pueden utilizarse para las transferencias de datos.

Prepararse para el cumplimiento del RGPD

Hay claramente una serie de áreas clave a observar en su enfoque para asegurar el cumplimiento del RGPD. Muchas obligaciones se pueden resolver de manera bastante sencilla y rápida. Otras, en concreto en organizaciones grandes y complejas, podrían tener importantes implicaciones presupuestarias, de IT, de personal, de regulaciones y de comunicaciones. Asegurar la participación de la alta dirección y las partes interesadas en su organización será crucial para cumplir sus obligaciones.

Un paso siguiente importante será, para la mayoría de las organizaciones, obtener claridad en su tratamiento de datos personales, e incluye identificar:

- Qué datos personales se conservan a lo largo de la organización
- Qué permisos se han obtenido para esos datos
- Qué procesos y sistemas están implantados para el tratamiento de los datos personales
- Cuando los datos personales se transfieren fuera de la organización (incluidos países terceros y transfronterizos)
- Cómo los datos personales se aseguran a lo largo de su ciclo de vida

Con un entendimiento de las lagunas de cumplimiento, las organizaciones estarán en situación de evaluar sus riesgos de datos personales y desarrollar un plan de remedio adecuado.

El momento de empezar a planificar el cumplimiento del RGPD es ahora.

Cómo podemos ayudar

Una autoridad global líder en la protección de datos, IT Governance ayuda a las organizaciones a que afronten los retos del cumplimiento del RGPD con un conjunto exhaustivo de recursos de información, soluciones y servicios de asesoría.

Servicios y soluciones de cumplimiento del RGPD			
Recursos de información	**Librería del RGPD**		
	RGPD UE – una guía de bolsillo	RGPD UE – una guía de implementación y cumplimiento	
Formación	**Cursos de formación en el RGPD**		
	• Iniciación certificada al RGPD • Profesional experto certificado al RGPD • Introducción y profesional combinado al RGPD		
	Aula	En directo por internet	Educación a distancia
Herramientas de cumplimiento	**Herramientas del RGPD**		
	Herramienta de documentación sobre RGPD UE		
Asesoramiento y consultoría	**Servicios de transición para el RGPD**		
	Auditoría del flujo de datos	Análisis de las diferencias del RGPD	Transición al RGPD
Certificación	**Sistema de gestión de la seguridad de la información**		
	Certificación ISO 27001		

Acerca del autor

Alan Calder es un reconocido gurú de ciberseguridad internacional y autor líder en seguridad de la información y cuestiones de regulaciones de TI. Además, es director ejecutivo de IT Governance Limited, el proveedor de fuente única de productos y servicios sobre regulaciones referidas a TI, gestión de riesgos y el sector del cumplimiento.

Alan escribió la guía de cumplimiento definitiva, *IT Governance: Una guía internacional para la seguridad de datos e ISO 27001/ISO 27002* (coescrito con Steve Watkins), que es la base para el curso de posgrado de la Universidad Abierta del Reino Unido sobre seguridad de la información. Este trabajo explica su experiencia de liderar la primera implementación con éxito del mundo de la BS 7799 (ahora ISO 27001).

Alan es un comentarista frecuente en medios de comunicación sobre la seguridad de la información y las cuestiones de regulaciones de TI y ha contribuido con artículos y comentario especializado en un amplio abanico de medios informativos nacionales, por internet y de la industria.

Servicios y productos de cumplimiento del RGPD

Libros

- **Reglamento General de Protección de Datos (RGPD) de la UE - Una guía de bolsillo**
  La perfecta introducción a los principios de la privacidad de los datos y el RGPD. Esta guía concisa es una lectura esencial para cualquiera que quiera obtener una visión de conjunto sobre las nuevas obligaciones de cumplimiento para tratar los datos personales de los residentes de la UE. La guía también está disponible en inglés, francés, alemán e italiano.
  Haga clic para obtener más información y para comprar el libro >>

- **Reglamento General de Protección de Datos de la UE (RGPD) – una guía de cumplimiento e implementación**
  Esta guía clara y exhaustiva ofrece un comentario pormenorizado sobre el RGPD y asesoramiento sobre la implementación práctica de las medidas de cumplimiento necesarias para su protección de datos y los regímenes de seguridad de la información.
  Haga clic para obtener más información y para comprar el libro >>

Cursos de formación

- **Curso de iniciación certificado sobre el RGPD UE**

  Este curso de un día le ofrecerá una sólida introducción al Reglamento General de Protección de Datos Europeo y le proporcionará un entendimiento práctico de las implicaciones y requisitos legales del Reglamento, culminando con una certificación oficial de la International Board of IT Governance Qualifications (IBITGQ).

  Haga clic para obtener más información y para reservar un curso >>

- **Curso profesional experto sobre el RGPD UE**

  Este exhaustivo curso de formación prepara aquellas personas que estén buscando incorporar su conocimiento del RGPD UE con el fin de poder ayudar al delegado de protección de datos de su organización (DPO por sus siglas en inglés). El curso cubrirá aspectos del Reglamento en profundidad, incluidos los requisitos de la implementación, las políticas y procesos necesarios, así como los métodos de análisis de los riesgos de seguridad de los datos.

  Haga clic para obtener más información y para reservar un curso >>

- **Curso de introducción y experto combinado sobre el RGPD UE**

  Este completo curso de formación te dará una visión completa sobre la nueva normativa de protección de datos. Es un curso de cinco días de duración en el que en el primero se tratarán todos los aspectos esenciales sobre el Reglamento. Durante los siguientes cuatro días se profundizará en todos los aspectos RGPD y en la figura del Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés).

  Haga clic para obtener más información y para reservar un curso >>

Herramientas de documentación

- **Herramienta de documentación sobre RGPD UE**

  Un conjunto completo de políticas y procedimientos que le permiten a su organización cumplir el RGPD UE. Estas plantillas digitales son totalmente personalizables y reducen considerablemente la carga de desarrollar los documentos necesarios para lograr el cumplimiento legal.

  Haga clic para obtener más información y para descargar una versión de prueba >>

Asesoramiento y consultoría

- **Auditoría del flujo de datos del RGPD**

  Para este primer paso fundamental en la preparación del proceso, nuestros expertos en privacidad le ofrecen un inventario de datos y un mapa de flujo de los datos personales conservados y compartidos por su organización. Esto forma la base para evaluar la privacidad de la información y los riesgos de seguridad en su organización.

  Análisis de las diferencias del RGPD

  Ofreciendo una evaluación específica de su cumplimiento con el RGPD, nuestros expertos en privacidad le ofrecen una evaluación detallada de su preparación, las diferencias y los riesgos clave y una hoja de ruta para el remedio.

  Haga clic para obtener más información y para ponerse en contacto con IT Governance para recibir asistencia >>

Certificación

- **Sistema de gestión de la seguridad de la información: ISO 27001**

  Reconocida internacionalmente como una manera eficaz de demostrar que las "medidas técnicas y organizativas adecuadas se han implementado" para cumplir con los requisitos del RGPD, nuestros

especialistas líderes en implementación de la ISO 27001 ayudarán a su organización a lograr la certificación.

Póngase en contacto con IT Governance para asistencia en servicecentre@itgovernance.eu >>

Soluciones de IT Governance

IT Governance consigue, crea y entrega productos y servicios para satisfacer las necesidades de regulación de TI en constante cambio de las organizaciones, directores, gerentes y profesionales de la actualidad.

IT Governance es su solución integral para la información, libros, herramientas, formación y consultoría corporativa y de regulaciones de TI. Nuestros productos y servicios son únicos en el sentido de que todos los elementos están diseñados para trabajar juntos armoniosamente para que pueda beneficiarse de estos individualmente o combinar los distintos elementos para crear algo más grande y mejor.

Nuestro enfoque **Proteger - Cumplir - Esforzarse** está dirigido a ayudar a que su organización logre resistencia ante el constante cambio.

Nuestras áreas de especialidad: