



RGPD

#ProtejoLosDatos

Comparte el mensaje.
Comparte la responsabilidad.

RESUMEN

RGPD

¿Conoces el RGPD? Es el cambio normativo más importante de los últimos 20 años en materia de protección de datos y viene a sustituir a la ya obsoleta LOPD. Este nuevo reglamento es de obligado cumplimiento y es de aplicación a partir del 25 de Mayo a todas las empresas de cualquier tamaño y sector con una normativa más exigente e imperativa. Por tanto, tienes ya sólo dos meses para adaptar tus procesos y las herramientas que gestionan información sensible.

Se está publicando mucha información del RGPD en Internet, pero pocas personas entienden las verdaderas implicaciones que tienen. La reglamentación no es fácil de entender para los no profanos, pero hay una cosa clara: esta nueva regulación es mucho más estricta e incorpora dos elementos importantes que debes conocer:

- Es de obligado cumplimiento para todas las empresas que venden en Europa independientemente del tamaño o sector, pudiendo recibir sanciones del 4% de tu facturación anual o 20 millones de euros (lo que sea mayor)
- Requiere proactividad por parte de las empresas, pudiendo recibir sanciones aún en casos de que no haya pérdida en sí de datos privados si se detecta que no se han puesto en marcha las medidas adecuadas según el estado de la técnica

Y no es tan sólo un riesgo económico directo, sino además un reto reputacional muy serio, ya que podríamos estar expuestos a demandas colectivas e incluso a la suspensión del tratamiento de datos por parte del regulador.

El cumplimiento con RGPD suponen unas exigencias que has primero entender bien y luego saber adaptar las herramientas y procesos que usas actualmente porque tendrás que cambiar algunas cosas que haces hoy en día.

Por ejemplo: ¿sabes que a partir del 25 de Mayo necesitarás recoger (y guardar de forma segura) el consentimiento de todos tus clientes para usar sus datos? ¿sabes que tendrás que avisar en menos de 72 horas desde que tengas una amenaza o fuga de

RESUMEN

RGPD

(...)

información sensible? ¿sabes que no podrás almacenar y enviar ficheros con información sensible de cualquier manera?

Sage está RGPD Ready

Por eso, en Sage hemos acometido una profunda transformación de nuestros productos, incorporando la nueva reglamentación de RGPD ya desde su diseño inicial. Así, nuestra solución Sage 50cloud | Sage 200cloud | SD4L incorpora sobre la plataforma algunas funcionalidades tan importantes como: gestión de consentimientos, revocaciones y derecho de acceso, gestión documental de información privada, trazabilidad del estado e histórico de actuación sobre la información sensible, herramientas de búsqueda y gestión de datos protegidos, informes y cuadros resumen de información marcada como protegida, etc.

Además, hemos creado un paquete formativo enfocado no solamente a que entiendas la nueva reglamentación; sino que entiendas, de una forma totalmente práctica y aplicable a tu negocio, cuales son las medidas que tienes que seguir para estar dentro del RGPD.

Es necesario que actualices tu aplicación si quieres asegurar que la información sensible de tu negocio y tus clientes que se gestiona dentro del software de gestión está bajo la reglamentación de RGPD.

Llamada a la acción

El RGPD es muy claro al respecto, es la empresa la responsable de asegurar que se han implementado las técnicas adecuadas; no siendo posible delegar esta responsabilidad a terceras partes. Por eso, es importante que asegures que cualquier software o sistema que gestiona información sensible este conforme al RGPD e incorpore funcionalidades que te ayuden en la gestión del día a día.

De lo contrario, la entrada en vigor del RGPD no sólo será un riesgo para tu negocio; sino que será imposible de gestionar de una forma eficiente.

RGPD



Capítulo 1

¿QUÉ ES EL RGPD? ¿CUÁL ES SU OBJETIVO?

RGPD

El RGPD (Reglamento General de Protección de Datos) o GRPD en sus siglas en inglés, es la última y más profunda reforma de la regulación europea en materia de protección de datos.

Su objetivo es armonizar los derechos de las personas, sean físicas o jurídicas, respecto a la gestión de los datos que ceden de forma consentida a las empresas; de forma que haya mucho más orden y control sobre cómo esa información es utilizada por las empresas.

La intención de la UE es devolver el control de la información personal a los propios usuarios; cosa que se ha perdido en los últimos años desde la explosión de Internet y los servicios digitales. La llamada transformación digital ha hecho que sea mucho más difícil garantizar la privacidad, ya que constantemente estamos cediendo todo tipo de información personal: nombres, direcciones, números de teléfono o de tarjetas de crédito en Internet; y muchas veces se hace de forma totalmente inconsciente y no consentida.

Por ejemplo, sólo en una visita a una web desde el móvil ya estás cediendo una gran cantidad de información que, en ocasiones, incluso contiene datos personales sin nuestro propio consentimiento; y no existe ningún control en cómo esta información es utilizada ni durante cuánto tiempo puede ser utilizada.

La LOPD, aun siendo una normativa muy estricta con respecto a las que han desarrollado otros países en EU, no se ajusta al mundo digital actual y no es suficiente para proteger la privacidad de los usuarios. Con RGPD, los ciudadanos están mejor protegidos contra el abuso y tienen más derechos en términos de protección de sus datos personales. RGPD no tiene la intención de prohibir la recopilación de datos, sino que garantiza que los intereses de los ciudadanos estén protegidos y que, si existe recogida de información de carácter personal, ésta se haga con un objetivo legítimo y de una forma totalmente transparente y ordenada.

Capítulo 1

¿QUÉ ES EL RGPD? ¿CUÁL ES SU OBJETIVO?

RGPD

(...)

Por eso RGPD incorpora el principio de transparencia en cuanto al derecho de los afectados a ser informados sobre el tratamiento de datos y contempla de forma expresa los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición al acceso a los datos personales por parte de las empresas.

En definitiva, RGPD es el mayor cambio legislativo europeo en los últimos 20 años; reemplaza a la Directiva de Protección de Datos de 1995, y supera a nuestra ya exigente LOPD. Su objetivo es defender la privacidad de todos los ciudadanos de la UE en su actividad online, protegiéndolos de los intereses comerciales -en muchas ocasiones, desmesurados- de las grandes compañías que operan en la Red.

Capítulo 2

¿QUÉ ES ESO DEL COMPLIANCE? ¿POR QUÉ DECÍS QUE ES IMPORTANTE?

RGPD

El compliance no es más que el aseguramiento de que los procesos en tu empresa cumplen con el marco regulatorio vigente en cada momento; y el RGPD es un importante cambio regulatorio.

El RGPD es una de las mayores reestructuraciones de cómo debería ser el tratamiento de los datos personales y puede llegar a afectar no solo a las empresas, sino a cualquier persona, entidad, autoridad pública, servicio u otro organismo que procese datos personales de quienes residan en la UE. Ahí se incluyen proveedores y terceras empresas a los que se encargue el tratamiento de datos personales.

Su ámbito de aplicación es muy amplio: todos los Estados de la UE, así como el Reino Unido tras su salida (Brexit) de la UE en 2019, ya que el RGPD también se incorporará a la legislación británica.

RGPD es la respuesta de la UE a los cambios provocados por la transformación digital, y supone la modernización más profunda de las leyes de protección de datos y los derechos de privacidad individuales de los últimos 20 años; regulando la recopilación, el almacenamiento, el uso y el intercambio de datos personales.

Capítulo 3

¿CUÁNDO ENTRA EN VIGOR ESTA NUEVA NORMATIVA? ¿ES OBLIGATORIA? ¿QUÉ SUCEDE SI NO LO HAGO?

RGPD

RGPD es una normativa aprobada por la Unión Europea el pasado 25 de mayo de 2016, si bien su aplicación real no será obligatoria hasta el 25 de Mayo de 2018, cuando sea traspuesta al ordenamiento jurídico español. Este periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que las empresas que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

Por tanto, estamos ya en la recta final del RGPD que es de obligado cumplimiento el día 25 de Mayo de 2018 para todas las empresas que prestan servicios a personas en territorio europeo.

El nuevo RGPD es una norma más estricta y no hace distinciones entre tamaños de empresa o sectores. Es una normativa de obligado cumplimiento, con sanciones a las empresas que pueden llegar al 4% de la facturación anual mundial o a los 20 millones de euros (lo que sea mayor); en caso de infracciones en materia de, entre otros aspectos, medidas técnicas y organizativas para la protección de datos, mantenimiento de registros, notificación de violaciones de seguridad de los datos personales y obligaciones de evaluación de impacto relativa a la protección de los mismos.

Además, la condena podrá imponerse, aunque no haya pérdida en sí de los datos; si se detecta que no se han puesto en marcha las medidas adecuadas para gestionar la información privada acorde a la normativa

Y no es tan sólo un riesgo económico directo, sino además un reto reputacional muy serio, ya que podríamos estar expuestos a demandas colectivas e incluso a la suspensión del tratamiento de datos por parte del regulador

**¿ES UNA LOPD
ACTUALIZADA?
¿SEGUIRÁ VIGENTE
LA LOPD DESPUÉS DE
LA ENTRADA EN VIGOR
DEL RGPD?**

RGPD

La LOPD, aun siendo una normativa más estricta que las de otros países en la UE, ha quedado obsoleta y no se ajusta al mundo digital actual. Hasta la entrada en vigor del RGPD, tanto la Directiva 95/46/CE como las normas internas de los diferentes países de la UE seguirán siendo aplicables, incluida la LOPD en España.

Por tanto, desde el punto de vista España, podemos pensar en el RGPD como una modificación de la actual Ley Orgánica de Protección de Datos, y que recogerá las modificaciones introducidas en cuanto a derechos, obligaciones, seguridad, etc. incorporadas en el Reglamento de la UE.

Capítulo 5

ESTO ES COMO LA LOPD, AL FINAL NADIE HARÁ CASO A ESTA NORMA. ¿POR QUÉ ESTO ES DIFERENTE Y TODO EL MUNDO ESTÁ HABLANDO DE ELLO?

RGPD

La gran cantidad de fuentes de información, el creciente volumen de datos que se gestiona cada día en una empresa, el crecimiento de las amenazas en cuanto a ciberseguridad y la preocupación de los ciudadanos por el uso que se hace de sus datos personales ha obligado a la UE a armonizar la legislación y a las empresas a revisar sus protocolos a través del RGPD.

Su aplicación afecta a todas las empresas, independientemente de su tamaño y sector de actividad, y supone el cambio más importante en cuanto a la protección de datos de los últimos 20 años; con un matiz que lo diferencia mucho de normativas anteriores: RGPD apela a la proactividad de las propias empresas. Es decir, las empresas están obligadas a poner las medidas preventivas de protección de datos acorde con el estado de la técnica; de lo contrario están incumpliendo de forma automática la normativa de RGPD.

Por tanto, el RGPD exige un mayor compromiso de las organizaciones, sean públicas o privadas, con la protección de datos incorporando una serie de nuevas obligaciones e, incluso, figuras dentro de las empresas que deben acometerse cuanto antes.

Así, por ejemplo, será necesario tener una nueva figura en la empresa denominada Delegado de Privacidad (DPO) en todos aquellos organismos públicos y empresas que gestionen grandes cantidades de datos; así como hacer un estudio de riesgos (Privacy Impact Assessment) para ser ellos mismos los que identifiquen posibles fallos o áreas de incumplimiento.

Además, el Reglamento exige que los responsables de tratamiento faciliten a los interesados el ejercicio de sus derechos; por lo que todas las empresas tienen que revisar sus avisos de privacidad y dotarlos de más claridad. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados puede dirigir sus reclamaciones a las Autoridades de protección de datos. Es importante recordar que el Reglamento exige de forma expresa que la información que se proporcione sea fácil de entender y presentarse en un lenguaje claro y conciso.

Capítulo 5

ESTO ES COMO LA LOPD, AL FINAL NADIE HARÁ CASO A ESTA NORMA. ¿POR QUÉ ESTO ES DIFERENTE Y TODO EL MUNDO ESTÁ HABLANDO DE ELLO?

RGPD

(...)

También es necesario diseñar e implantar los procedimientos para notificar adecuadamente a las Autoridades de protección de datos o a los interesados las quiebras de seguridad que pudieran producirse.

Todos estos cambios no serán un problema para las grandes empresas, ya que cuentan con expertos a nivel de gestión de datos tanto a nivel técnico como legal. Sin embargo, son las pequeñas y medianas empresas las que más complicada van a tener su aplicación si no buscan el apoyo de un socio tecnológico, pues se les exige la misma proactividad para implementar las medidas de seguridad y de protección de la información conforme al estado de la técnica.

En general, cualquier empresa que trata datos personales está obligada a preparar, antes del 25 de Mayo, todas sus aplicaciones que gestionan información sensible conforme al nuevo Reglamento de RGPD.

Capítulo 6

¿QUÉ SIGNIFICA ESO DE RESPONSABILIDAD ACTIVA? ¿EN QUÉ ME AFECTA?

RGPD

El RGPD supone una mejora de los derechos de privacidad de los ciudadanos; pero trae consigo un aumento en las obligaciones para las empresas en referencia a la gestión de esa información privada.

Uno de los aspectos esenciales del RGPD, y que lo diferencia totalmente de cualquier normativa anterior, es el de la "responsabilidad activa". Así, las empresas están obligadas a adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD establece. El reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

En ese sentido, el RGPD exige a las empresas la proactividad o "responsabilidad activa", y que tomen medidas para la protección de datos desde el propio diseño de sus aplicaciones y sistemas, incorporando medidas de gestión de datos y de seguridad adecuadas y llevando un registro de todos los tratamientos realizados para asegurar la información de sus usuarios. Además, y esta es una de las grandes novedades, las empresas deberán notificar públicamente cuando se produzca una violación de la seguridad de los datos. Concretamente, las empresas están obligadas a notificar brechas de seguridad en un plazo máximo de 72 horas

En definitiva, las organizaciones deben prepararse desde ya mismo para una nueva responsabilidad proactiva, no reactiva. De no hacerlo, se exponen a sanciones que pueden alcanzar los 20 millones de euros o el 4% de la facturación global. La cifra que resulte mayor de ambas.

Capítulo 7

¿QUIÉN TIENE QUE CUMPLIR CON EL RGPD? ¿AFECTA A TODOS LOS SECTORES Y TODOS LOS TAMAÑOS DE EMPRESA? ¿EN QUÉ AFECTA A EMPRESAS COMO YO EL RGPD?

RGPD

El Reglamento se aplicará a empresas establecidas en la Unión Europea, pero se amplía ahora a empresas no establecidos en la UE siempre que presten servicios a ciudadanos y otras empresas de la UE. Por tanto, tiene grandes implicaciones para todos los departamentos de muchas compañías a nivel mundial, afectando a las empresas y a quienes se encarguen del tratamiento de datos para ellas (incluso fuera de la UE).

Para que esta ampliación del ámbito de aplicación pueda hacerse efectiva, esas organizaciones deberán nombrar un representante en la Unión Europea, que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos y que, en caso necesario, podrá ser destinatario de las acciones de supervisión que desarrollen esas autoridades. Los datos de contacto de ese representante en la Unión deberán proporcionarse a los interesados entre la información relativa a los tratamientos de sus datos personales.

RGPD obliga a las empresas a revisar los procesos asociados a la gestión de datos personales, tanto en términos de seguridad como de almacenamiento y tratamiento. Esto quiere decir que tiene implicaciones importantes para todos los departamentos de muchas compañías de todo el mundo; siendo necesario en algunos casos incluso contratar o designar un delegado de protección de datos.

Estos son los puntos de partida del RGPD para su correcto cumplimiento:

- Solo puedes usar aquellos datos personales que estén respaldados por un uso legítimo, y solo para el propósito para el cual se recopiló originariamente la información. Por tanto, es necesario contar con el consentimiento explícito del usuario y, además, ese consentimiento será ahora revocable en cualquier momento.
- Debes saber exactamente qué información de carácter personal tienes en tu poder y qué datos contienen
- Debes especificar cómo garantizas la seguridad cuando procesas datos personales; estando obligado a notificar cualquier fallo de seguridad en un plazo de 72 horas a la Agencia Española de Protección de Datos.

Capítulo 7

¿QUIÉN TIENE QUE CUMPLIR CON EL RGPD? ¿AFECTA A TODOS LOS SECTORES Y TODOS LOS TAMAÑOS DE EMPRESA? ¿EN QUÉ AFECTA A EMPRESAS COMO YO EL RGPD?

RGPD

(...)

- Debes saber qué derechos tienen los sujetos de datos, aquellas personas cuyos datos personales se tratan, y permitirles ejercerlo cuando lo soliciten
- Para los proyectos en los que trabajas con datos personales, debes realizar previamente una evaluación de los riesgos, llamada evaluación de Impacto de la Privacidad (DPIA por sus siglas en inglés)
- Es posible que necesites designar un Delegado de Protección de Datos
- Debes poder garantizar la confidencialidad, la integridad, la disponibilidad y la robustez de tus sistemas y servicios que traten datos personales.

Te vamos a nombrar algunos Ejemplos cotidianos de una empresa y cómo están afectados por el RGPD:

Empleados.

En cualquier proceso de selección de personal, deberás aplicar los artículos del RGPD relacionados con el Consentimiento de tu candidato al uso de sus datos personales que recabes y guardes. Recuerda que un papel que los recoja ya es objeto a ser protegido y en su caso, destruido pasado el proceso de captación.

Debes informar del tiempo en el que dispondrás de sus datos personales para en su caso, pasado el periodo de selección, anonimizarlo o destruido. Ten en cuenta que, si no lo tienes en cuenta, la persona puede solicitarlo posteriormente. Debes disponer de herramientas que te ayuden a este proceso.

Si este candidato pasa a empleado y por contrato Consiente a lo que tu empresa disponga para ese momento de firma/ consentimiento (derechos de imagen a su uso, a que sus datos de identidad puedan ser visibles, para temas relacionados con cámaras de seguridad, a controles de acceso, etc., recuerda que debes almacenar y custodiarlas adecuadamente.

Pero si a la firma de ese contrato de trabajo no se recogen otro tipo de consentimientos como el poder disponer de incentivos especiales relacionados con premios, concursos, viajes, etc., o a que sus datos sean usados por terceros o en cualquier otro tipo de actividad que no esté estipulada bajo contrato y se usen

Capítulo 7

¿QUIÉN TIENE QUE CUMPLIR CON EL RGPD? ¿AFECTA A TODOS LOS SECTORES Y TODOS LOS TAMAÑOS DE EMPRESA? ¿EN QUÉ AFECTA A EMPRESAS COMO YO EL RGPD?

RGPD

(...)

su datos personales, deberás disponer de su Consentimiento Expreso para cada caso y temporalidad, con todo lo que comporta documentalmente y la gestión de los vencimientos de cada consentimiento.

Si además gestionas datos sensibles adicionalmente a los personales como partes de accidente, situaciones médicas, de estado civil, tendencias políticas o de creencia o afiliación sindical, etc., estos datos deberán ser protegidos en grado máximo.

Finalmente, si tienes una rotación alta de personal, deberás estar preparado para gestionar y aplicar solicitudes de Derecho al Olvido o Portabilidad de información.

Prospección comercial (Potencial cliente).

Recabas información en vistas puerta fría, ferias o congresos, en acciones online con formulario de inscripción o cumplimentación de datos, etc.

En la mayoría de los casos, las acciones de contacto face to face se hacen entre personas, por lo que los primeros datos recogidos contienen un contacto con datos personales a quienes posteriormente te servirán para iniciar tu proyecto empresarial.

Debes solicitar un Consentimiento expreso a ese contacto previo a cualquier actividad. Lo debes recoger, almacenar y custodiar. Ya puedes seguir con tus acciones de relación. Pero si amplías nuevos contactos y vas a generar nuevas vías de relación, recuerda que debes solicitar sus consentimientos previamente.

Si esa relación comercial, prospera para ser un cliente habitual a quien facturas, tu relación cambia y deberás disponer de un documento (contrato o anexos de consentimientos) que avalen el uso de los datos personales de las personas con las que estarás en contacto. Si alguna de estas personas es sustituida por otra, deberías tener una notificación por parte de la empresa o bien recabar de nuevo su consentimiento previo.

Recuerda que estas relaciones comerciales se extienden a colaboradores (agentes ciales por cuenta propia, Transportistas o empleados de las mismas, terceras empresas que te hacen tareas de limpieza, acciones de TLMK, paquetería, etc.)

Capítulo 7

¿QUIÉN TIENE QUE CUMPLIR CON EL RGPD? ¿AFECTA A TODOS LOS SECTORES Y TODOS LOS TAMAÑOS DE EMPRESA? ¿EN QUÉ AFECTA A EMPRESAS COMO YO EL RGPD?

RGPD

(...)

Si la captación de datos personales se realiza bajo formulario digital, deberás mostrar claramente e inequívocamente en dicho formulario todo lo referente a obtener el consentimiento de tu nuevo contacto, así como informarle de todo lo relacionado con lo referente relacionado con el RGPD. Esos datos deberán depositarse en una BBDD o en tu ERP teniendo el mismo circuito de almacenamiento y custodia que si fuese introducido manualmente.

En cualquier caso, desde Sage recomendamos encarecidamente que las personas adecuadas en cada organización se formen no sólo a nivel teórico sobre RGPD; sino a nivel práctico para entender bien las implicaciones e impacto del RGPD, así como estudiar cual es la aplicación concreta en su empresa.

Las Soluciones Avanzadas RGPD Ready de Sage, disponen de funcionales específicas para la gestión de Consentimientos, revocaciones, derecho al olvido, transferencias de información, etc.

En resumen, **si tu empresa trabaja con datos personales de ciudadanos de la Unión Europea, a partir del 25 de mayo de 2018 estarás obligado a cumplir con el nuevo RGPD.**

RGPD es una normativa que requiere un cierto esfuerzo, implicación y proactividad para su correcta implementación. En el caso de una gran empresa, como Sage, se están poniendo en marcha proyectos específicos para la implementación de RGPD; donde se involucra a todos los Departamentos y se suele colaborar con una empresa de consultoría especializada. Sin embargo, una PYME no tiene el tiempo ni los recursos para ello. Y es ahí donde Sage quiere dar una solución; evitando que estas pequeñas y medianas empresas puedan resultar sancionadas por una incorrecta interpretación o implantación de esta normativa.

De lo contrario, se exponen a la posibilidad de incurrir en una sanción de hasta el 4 % del volumen de negocio anual en todo el mundo o de 20 millones de euros (la que sea de mayor cuantía), simplemente por un desconocimiento de qué es y cómo se cumplen con la normativa de RGPD.

NO ENTIENDO ESTO DEL RGPD, ¿QUÉ ESTÁN HACIENDO EL RESTO DE EMPRESAS EN ESTE MOMENTO?

RGPD

Tranquilo, no eres el único que tiene dudas. De hecho, según un estudio realizado por IDC y Microsoft respecto al RGPD revela que, a escasos 2 meses para que entre en vigor el RGPD, solo el 10% de la empresa española está preparada para implantarlo de forma correcta; estando muy por debajo de otros países como Alemania o UK que están más cerca del 25%. Sin embargo, sólo un 20% de empresas reconoce abiertamente que no tiene ningún plan para abordarlo o está a la espera de más información.

Esto quiere decir que, con los esfuerzos de difusión por parte la Administración Pública y una fecha clara de entrada en vigor a la normativa; las empresas son conscientes de que tienen que aplicar un plan. El problema es que todavía existe mucha confusión sobre cómo puede cumplirse con esta nueva normativa.

Sin embargo, pese a esta conclusión claramente pesimista, el estudio refleja que las empresas sí entienden una cosa del RGPD: requiere hacer cambios y es de obligado cumplimiento. Y por eso el estudio refleja que la inversión de las empresas españolas para adaptar sus procesos y sistemas al RGPD se incrementará este año un 44% respecto a 2017. De todas las partidas presupuestarias, las que más van a crecer son las destinadas a la revisión y mejora de la gestión de identidades y el acceso a la información (70%), la actualización de aplicaciones que usen datos privados a los que es necesario aplicar RGPD (66%) y la comunicación interna y formación de empleados (61%).

Por eso, se recomienda recibir la formación adecuada en esta nueva normativa de protección de datos para trabajar con tiempo en los cambios necesarios para llevar a cabo una correcta adaptación (y evitar posibles sanciones). Además, de tener un software que os ayude a llevar a cabo las exigencias que exige el reglamento para que os sea mucho más fácil y ágil su gestión diaria.

Capítulo 9

¿QUÉ TENGO QUE HACER PARA ADECUARME AL RGPD? ¿QUÉ ME RECOMENDÁIS QUE HAGA ENTONCES PARA IMPLEMENTAR EL RGPD?

RGPD

Un primer paso recomendable sería visitar la zona del sitio web de la AEPD dedicada al nuevo Reglamento General de Protección de Datos, donde podrás encontrar varias guías e información general. En concreto, consulta la publicación de la AEPD, «Guía del Reglamento General de Protección de Datos para responsables del tratamiento».

Como todo cambio legal, el RGPD puede parecer más problemático de lo que es en realidad. Sin embargo, con una buena comprensión de las implicaciones y el uso de herramientas adecuadas no debería ser un gran problema el cumplimiento de dicha normativa.

Los cambios y procesos a revisar en cualquier empresa pueden resumirse en:

- **Consentimiento:** debe ser una declaración u otra acción afirmativa clara. No se puede dar por supuesto ni siquiera usar casillas ya marcadas en una web.
- **Delegado de protección de datos:** puede ser obligatorio. Debe estar especializado en la legislación de protección de datos. Puede ser empleado o subcontratado.
- **Privacidad de principio a fin:** la privacidad debe tenerse en cuenta en todo y solo pueden usarse los datos estrictamente necesarios para el fin estipulado.
- **Ámbito de aplicación mayor:** afecta a las empresas y a quienes se encarguen del tratamiento de datos para ellas, incluso fuera de la UE.
- **Comunicación obligatoria de las violaciones de la seguridad:** los responsables de los datos deben informar a la autoridad de control (la AEPD en España) en el plazo de 72 horas desde su conocimiento. En violaciones graves de la seguridad, hay que informar a los interesados
- **Portabilidad de los datos:** las personas tienen ahora el derecho a mover, copiar o transferir sus datos, incluso a una empresa de la competencia.

Capítulo 9

¿QUÉ TENGO QUE HACER PARA ADECUARME AL RGPD? ¿QUÉ ME RECOMENDÁIS QUE HAGA ENTONCES PARA IMPLEMENTAR EL RGPD?

RGPD

(...)

- **Sanciones:** pueden llegar al 4 % de la facturación anual global del ejercicio anterior o 20 millones de euros, lo que sea mayor (frente a los 300.000€ como máximo de lo que hay actualmente con la LOPD). La sanción puede imponerse, aunque no haya pérdida en sí de los datos.

Pero esto no implica necesariamente ni en todos los casos una mayor carga. En muchos casos será sólo una forma de gestionar los datos distinta de la que se viene empleando ahora o el uso de herramientas software preparadas para ello.

En todos los casos, **el Reglamento prevé que la obligación de estas medidas**, o el modo en que se apliquen, dependerá de factores tales como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos. Por tanto, es vital concentrarse en acometer el tratamiento de la información más sensible en lugar de perderse en la maraña informática de una empresa.

Para ello, **es necesario que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus aplicaciones para poder determinar qué medidas han de aplicar y cómo hacerlo.** Estos análisis pueden ser operaciones muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen, por ejemplo, datos sensibles, u operaciones más complejas en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que por sus características requieren de una valoración cuidadosa de sus riesgos.

A partir de ahí, te recomendamos que revises tus aplicaciones y sistemas de captura, almacenamiento y tratamiento de datos personales para asegurarte de que sean conformes con el RGPD; incluyendo por supuesto el software de contabilidad y gestión que es quizá uno de los que más información sensible gestiona. Además, puedes pensar en realizar una auditoría de RGPD desde los puntos de vista legal y tecnológico, aunque no es obligatoria.

Capítulo 9

¿QUÉ TENGO QUE HACER PARA ADECUARME AL RGPD? ¿QUÉ ME RECOMENDÁIS QUE HAGA ENTONCES PARA IMPLEMENTAR EL RGPD?

RGPD

(...)

Asegúrate de que tus empleados y colaboradores conozcan el RGPD y organiza cursos para que estén preparados. Recuerda que el RGPD también te hace responsable del tratamiento de datos personales que terceros hagan para ti.

Así, teniendo en cuenta el estado de la técnica (es decir, la tecnología disponible en este momento), el coste de la aplicación y la naturaleza y los riesgos asociados a la gestión de datos personales en tu negocio; serás tú quien decidas las medidas para garantizar de forma efectiva los principios de protección de datos del RGPD. En otras palabras, cada empresa tendrá que hacer cosas distintas, en función de los datos que gestione y las aplicaciones que utilice para ello.

Estas medidas harán referencia a cosas como la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Y todo eso, ¿qué significa? Pues como sucede con toda nueva regulación, ésta está sujeta a múltiples interpretaciones por parte de los expertos. Pero, en todas ellas, se incluye que las empresas deben incorporar medidas técnicas que protejan la privacidad en el propio diseño de los sistemas TIC y de las aplicaciones, así como a que solo se almacene o procese la cantidad mínima de datos personales que sean estrictamente necesarios.

En este sentido, el poder demostrar que se han tomado medidas para mejorar el cumplimiento es casi tan importante como el cumplimiento en sí mismo. Cualquier inversión o actualización en los sistemas que gestionan información privada o de carácter personal es un paso en este camino.

Sage te ayuda con todo lo anterior, para que no te pille de sorpresa este cambio tan exigente y estés preparado para afrontarlo de la manera más ágil y fácil, tanto en cuanto a formación de lo que debes hacer en el día a día de tu negocio como en cuanto a un producto para poder afrontar de manera fácil las exigencias de la norma.

Capítulo 10

¿CÓMO PUEDE SAGE AYUDARME EN ESTE PROCESO?

RGPD

El cumplimiento con RGPD supone una completa revisión de procedimientos dentro de la organización que afecta a la práctica totalidad de los departamentos. Independientemente del estado de transformación digital de tu empresa, el software y los sistemas TIC desempeñan un papel esencial en la preparación para el RGPD porque son al fin y al cabo las responsables del tratamiento de los datos.

Además, es importante no olvidar que el cumplimiento con el reglamento RGPD no es un hecho puntual que culmina el próximo 25 de mayo, cuando sea obligatorio a aplicarse el reglamento; sino más bien será un marco de trabajo que nos va a acompañar durante muchos años y es un camino que no debemos recorrer solos. Por eso es tan importante elegir bien tu socio en este viaje.

Sage se encuentra trabajando activamente en desarrollar herramientas y contenidos para ayudar a todos sus clientes en la implementación del RGPD. Sage cuenta con los mejores expertos en software legal y una experiencia de más de 40 años en el desarrollo y mantenimiento de software con alto contenido legal. Por tanto, contamos con procedimientos de control sólidos para incorporar funcionalidades en nuestros productos que faciliten la gestión del RGPD.

Capítulo 10

¿CÓMO PUEDE SAGE AYUDARME EN ESTE PROCESO?

RGPD

(...)

En una primera instancia, en Sage hemos puesto a disposición de nuestros clientes una herramienta de autoevaluación rápida y gratuita que sin recabar datos del usuario y tras contestar a unas sencillas preguntas, aporta un informe orientativo sobre los pasos y las tecnologías que se pueden implementar para el cumplimiento del RGPD.

Por otro lado, en Sage hemos desarrollado funcionalidades específicas en nuestras soluciones para que puedes mantenerte de forma más sencilla dentro de la legislación vigente. Las soluciones que proponemos abarcan de forma modular y complementaria las siguientes colecciones de herramientas, soluciones y servicios empresariales.

En este sentido, desde Sage recomendamos encarecidamente la actualización software a las versiones S50cloud, S200cloud o SD4L ya que incorporan las mejores prácticas que emanan del RGPD ya desde su diseño; ofreciendo todas las facilidades y herramientas para evitar que la implantación del RGPD se convierta en una pesadilla.

Además, hemos creado paquetes formativos que te ayudarán a entender a ti y al resto de empleados de tu empresa en que consiste la normativa y sí estáis gestionando la información de forma adecuada; dándoos las pautas para adecuar vuestra forma de trabajar a las nuevas reglas.

Desde Sage reiteramos nuestro compromiso con la gestión de información y la seguridad, y nuestra total confianza tanto en las tecnologías que proponemos como en la red de partners preparados para que nuestros clientes puedan asumir el cumplimiento de RGPD, gran protagonista de este año 2018.

Capítulo 11

HE LEÍDO QUE TENGO QUE PEDIR UN CONSENTIMIENTO A TODOS MIS CLIENTES PARA GESTIONAR SU INFORMACIÓN. ¿ESTO ES ASÍ?

RGPD

Una de las bases fundamentales para tratar datos personales es el consentimiento. RGPD pide que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es "inequívoco", el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

Las empresas deberían revisar la forma en la que obtienen y registran el consentimiento. Prácticas que se encuadran en el llamado consentimiento tácito y que son aceptadas bajo la actual normativa dejarán de serlo cuando el Reglamento sea de aplicación.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento. Por ello, es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

Aquí también Sage te puede ayudar a que este proceso resulte mucho más sencillo con el software que hemos desarrollado enlazado con la gestión documental para la gestión y control de la documentación exigida en el reglamento.

¿QUIÉN ES EL RESPONSABLE SI SE DETECTA ALGÚN NO-CUMPLIMIENTO? ¿QUÉ REPERCUSIONES PUEDE TENER PARA MÍ ESTO?

RGPD

El responsable siempre es la empresa

El nuevo RGPD será una norma más estricta. Las sanciones a las empresas pueden llegar al 4% de la facturación anual global del ejercicio anterior o a los 20 millones de euros (lo que sea mayor). Además, la condena podrá imponerse, aunque no haya pérdida en sí de los datos.

Con el nuevo RGPD, la empresa tiene, todavía, más responsabilidad y compromisos para dotarse de herramientas y aplicar procedimientos que cumplan con el nuevo Reglamento.

(Formar a sus empleados y colaboradores, usar software legal y preparado RGPD, aplicar servicios y seguridad para dar respuesta a las nuevas exigencias en estas materias, entre otros). Es la empresa quien debe conocer los alcances del RGPD en su negocio, es la empresa quien gestiona sus soluciones empresariales, quien conoce dónde guarda la información de datos personales de sus clientes, quién la usa y para qué, quien debe generar, enviar, almacenar y custodiar los Consentimientos de sus contactos o gestionar las peticiones de revocación / olvido de los datos personales de quien se lo pida y anonimizarlos cuando proceda o transferir estos datos a otras empresas o al propio contacto si se lo solicita.

Eso sólo lo puedes hacer tú desde dentro de tus sistemas. La empresa deberá demostrar que ha estado dotando a tu negocio de medios para proteger lo mejor posible los datos personales de tus contactos.

¿NECESITO TENER ALGÚN EXPERTO EN MI EMPRESA RESPECTO AL RGPD?

RGPD

El reglamento introduce la exigencia de nombrar un Delegado de Protección de Datos (DPO, Data Protection Officer) en varios supuestos:

- Ser organización del sector público
- Hacer analítica masiva de datos de ciudadanos
- Gestionar a gran escala datos sensibles de categorías especiales (raza, sexo, salud, religiosos, políticos, genéticos...).

Una de las tareas más importantes de este DPO será la de notificar las brechas de seguridad dentro de las 72 horas posteriores a su descubrimiento. Por ello, los controladores de datos deberán notificar a las autoridades de supervisión (en nuestro caso la Agencia Española de Protección de Datos) las violaciones de datos sin demoras indebidas. Adicionalmente los sujetos de datos también deberán ser notificados sin demora si la violación de datos personales representa un "alto riesgo" para sus derechos y libertades.

Capítulo 14

POR FAVOR, ¿PODRÍAS DEMOSTRARME CÓMO AYUDA SAGE AL CUMPLIMIENTO EL RGPD? NECESITO TENER LA SEGURIDAD DE QUE CUMPLO CON LA NUEVA NORMATIVA VIGENTE (ARTÍCULO POR ARTÍCULO)

RGPD

La verdad es que se están publicando muchos artículos y documentos sobre el RGPD, pero casi todos se quedan a un nivel general y no explican claramente las nuevas responsabilidades y, lo que es más importante, cómo resolverlas.

A continuación, te puedo dar algunos ejemplos concretos de cómo podemos ayudarte

Art. 24. Responsabilidad del responsable del tratamiento

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines el tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

- Software legal
- Recovery
- Portfolio de seguridad: Antivirus, antimalware
- Bases de datos en MSSQL
- Autorización de acceso por usuarios
- Seguridad en las contraseñas
- Restricción de acceso a usuarios en entidades de interesados según los datos
- Restricción de acceso a usuarios en entidades según su uso (ex. No ver nomina de una empresa de conta)

Capítulo 14

POR FAVOR, ¿PODRÍAS DEMOSTRARME CÓMO AYUDA SAGE AL CUMPLIMIENTO EL RGPD? NECESITO TENER LA SEGURIDAD DE QUE CUMPLO CON LA NUEVA NORMATIVA VIGENTE (ARTÍCULO POR ARTÍCULO)

RGPD

(...)

Art. 25 Protección de datos desde el diseño y por defecto

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

- Portfolio de formación RGPD Ready.
- Portfolio de seguridad: Antivirus, antimalware
- Bases de datos en MSSQL
- Autorización de acceso por usuarios
- Seguridad en las contraseñas
- Restricción de acceso a usuarios en entidades de interesados según los datos
- Restricción de acceso a usuarios en entidades según su uso (ex. No ver nomina de una empresa de conta)

Capítulo 14

**POR FAVOR, ¿PODRÍAS
DEMOSTRARME
CÓMO AYUDA SAGE
AL CUMPLIMIENTO
EL RGPD?
NECESITO TENER
LA SEGURIDAD DE QUE
CUMPLO CON LA NUEVA
NORMATIVA VIGENTE
(ARTÍCULO POR ARTÍCULO)**

RGPD

(...)

Art. 28 Encargado del tratamiento

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado

- Software legal
- Recovery
- Portfolio de seguridad: Antivirus, antimalware
- Bases de datos en MSSQL
- Autorización de acceso por usuarios
- Seguridad en las contraseñas
- Restricción de acceso a usuarios en entidades de interesados según los datos
- Restricción de acceso a usuarios en entidades según su uso (ex. No ver nomina de una empresa de conta)

Art 32. Seguridad del tratamiento

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

Capítulo 14

POR FAVOR, ¿PODRÍAS DEMOSTRARME CÓMO AYUDA SAGE AL CUMPLIMIENTO EL RGPD? NECESITO TENER LA SEGURIDAD DE QUE CUMPLO CON LA NUEVA NORMATIVA VIGENTE (ARTÍCULO POR ARTÍCULO)

RGPD

(...)

- Cifrado de datos (ocultación)
- Restricción de acceso a usuarios en entidades de interesados según los datos
- Recovery system: offering de seguridad
- Registro de actividad sobre un dato
- La seguridad en SQL

Tratamiento basado en el consentimiento del afectado.

De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

- Plantillas que facilitan la emisión del consentimiento
- Plantillas de facilitan la revocación del consentimiento
- Plantillas para gestionar el derecho al acceso
- Control del estado de las peticiones de consentimiento
- Almacenamiento en Gestión Documental de documentos emitidos y recibidos
- Registro de estado del consentimiento
- Fechas de vigencia del consentimiento
- Reporting de estados de consentimiento
- Información de los consentimientos por entidad (aceptación de uso para fines comerciales, autorización para la portabilidad de la información, autorización para la transferencia internacional de la información)
- Historico de registro de acciones realizadas sobre la entidad: Estados de informes generados (log)
- Informe del proposito de los datos según entidad
- Informe de registro histórico de actividades.

Capítulo 14

POR FAVOR, ¿PODRÍAS
DEMOSTRARME
CÓMO AYUDA SAGE
AL CUMPLIMIENTO
EL RGPD?
NECESITO TENER
LA SEGURIDAD DE QUE
CUMPLO CON LA NUEVA
NORMATIVA VIGENTE
(ARTÍCULO POR ARTÍCULO)

RGPD

(...)

Art. 17 Derecho de supresión o derecho al olvido

Gestinando las excepciones de obligaciones legales.

“para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable”

- Impresos oficiales que persisten el detalle de la información presentada

Art. 18 Derecho a la limitación del tratamiento

- Bloqueo de procesos en empresas
- Posibilidad de tratamiento de registros según el dato (campo)
- Información de los consentimientos por entidad (aceptación de uso para fines comerciales, autorización para la portabilidad de la información, autorización para la transferencia internacional de la información)

Art. 20. Derecho a la portabilidad de datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento o, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento

- Informes exportables a xls
- Exportación de datos en xls
- Exportación de datos csv

**¿TENGO QUE ESTAR
CERTIFICADO EN RGPD?
¿CÓMO LO HAGO?
¿ME AYUDA SAGE EN
ESTE PROCESO?**

RGPD

El reglamento de RGPD no menciona en ninguno de sus artículos la necesidad expresa de tener ningún tipo de certificado u homologación ninguna.

Lo que dice el nuevo reglamento es que las empresas tienen que ser proactivas, y no reactivas. Es decir, las empresas están obligadas a poner las medidas preventivas de protección de datos acorde con el estado de la técnica; de lo contrario están incumpliendo de forma automática la normativa de RGPD.

Y no especifica nada más al respecto ¿esto qué significa? Pues como sucede con toda nueva regulación, ésta está sujeta a múltiples interpretaciones por parte de los expertos. Pero, en todas ellas, se incluye que las empresas deben incorporar medidas técnicas que protejan la privacidad en el propio diseño de los sistemas TIC y de las aplicaciones, así como a que solo se almacene o procese la cantidad mínima de datos personales que sean estrictamente necesarios.

En este sentido, el poder demostrar que se han tomado medidas para mejorar el cumplimiento es casi tan importante como el cumplimiento en sí mismo. Cualquier inversión o actualización en los sistemas que gestionan información privada o de carácter personal es un paso en este camino.

¿QUÉ HACE VUESTRO MODULO SOFTWARE? ¿POR QUÉ LO NECESITO? EJEMPLO PRÁCTICO DE LO QUE HACE VUESTRA HERRAMIENTA

RGPD

En Sage hemos acometido una profunda transformación de nuestros nuevos productos, incorporando la nueva reglamentación de RGPD ya desde su diseño inicial. Así, nuestra solución Sage 50cloud | Sage 200cloud | SD4L incorpora sobre la plataforma algunas funcionalidades tan importantes como: gestión de consentimientos, revocaciones y derecho de acceso, gestión documental de información privada, trazabilidad del estado e histórico de actuación sobre la información sensible, herramientas de búsqueda y gestión de datos protegidos, informes y cuadros resumen de información marcada como protegida, etc.

Para ello, desplegamos una funcionalidad exclusiva que va a ayudar a cualquiera de nuestros clientes en la gestión y control de la documentación y datos que dispone de sus clientes con las siguientes características.

Gestión RGPD a nivel de Entidades principales:

En cada mantenimiento con información de datos protegidos, se habilitará una nueva opción que permitirá la gestión de la documentación a efectos del cumplimiento del RGPD, así como el control y gestión de las solicitudes y fechas RGPD.

Como Entidades principales entendemos: Clientes, Proveedores, Empleados, Cuentas Contables, ...) y entidades derivadas de las principales (potenciales, referencias, técnicos,...).

Capítulo 16

¿QUÉ HACE VUESTRO MODULO SOFTWARE? ¿POR QUÉ LO NECESITO? EJEMPLO PRÁCTICO DE LO QUE HACE VUESTRA HERRAMIENTA

RGPD

(...)

Las principales funcionalidades que dispondremos desde las diferentes entidades son:

- Generación de documentos para el tratamiento del consentimiento, revocación y derecho al acceso (con plantillas de envíos)
- Almacenamiento de los documentos emitidos y recibidos para poder ser consultados posteriormente.
- Control del estado de las diferentes peticiones realizadas (Fecha emisión, recepción, estado de la petición...)
- Identificación y registro de los consentimientos (aceptación de uso para fines comerciales, autorización para la portabilidad de la información, autorización para la transferencia internacional de la información)
- Gestión de fechas de retención de la información de carácter personal.
- Histórico de registro de las acciones realizadas sobre la entidad.
- Informe del propósito de los datos según entidad en la que estemos.
- Informe de registro histórico de actividades.
- Informe de identificación del tipo de información de datos protegidos que disponemos en la solución (Listado de propósito).

Se trata de un informe dinámico que ofrecerá información de que entidades tienen registros con información susceptible RGPD. La información será por empresas y entidades. Afecta a datos y campos estándares del producto.

Capítulo 16

¿QUÉ HACE VUESTRO MODULO SOFTWARE? ¿POR QUÉ LO NECESITO? EJEMPLO PRÁCTICO DE LO QUE HACE VUESTRA HERRAMIENTA

RGPD

(...)

Gestor RGPD:

El gestor RGPD será la herramienta que ayudará a nuestros clientes a gestionar y llevar el control de los datos personales con el objetivo de ayudarles a realizar el cumplimiento del RGPD.

Desde el gestor RGPD dispondremos de:

- Información teórica relacionada con el RGPD, así como recomendaciones sobre el uso del producto para el cumplimiento del RGPD.
- Visor de los campos protegidos y posibilidad de definir nuevos campos a efectos de contemplar las personalizaciones en la solución.
- Listado de propósito con las entidades y campos afectados que el cliente esté gestionando en la solución
- Ejecución de las acciones relacionadas con las entidades de forma masiva. Permitirá, por ejemplo, la generación del documento de consentimiento para un conjunto de registros.
- Herramienta de búsqueda de datos protegidos. Localizar en que entidades tenemos registrado un dato protegido
- Lista de registro de actividad. Listado del uso de la información marcada como dato protegido.
- Informe resumen de la situación de los consentimientos gestionados, emitidos y recibidos.
- Informe resumen de la situación de las revocaciones gestionadas, emitidas y recibidas.

Capítulo 16

¿QUÉ HACE VUESTRO MODULO SOFTWARE? ¿POR QUÉ LO NECESITO? EJEMPLO PRÁCTICO DE LO QUE HACE VUESTRA HERRAMIENTA

RGPD

(...)

En resumen, se ha definido una funcionalidad RGPD “llaves en mano” que contempla una gestión ágil, completa e integrada favoreciendo la productividad del despacho.

Con total información respecto a los campos con datos sensibles propios de la solución Sage Despachos; permitiendo ampliarlo a las adaptaciones que puedan tener algunos clientes con una configuración específica en cada caso.

La entrega de este contenido se realizará por fases hasta la entrada en vigor del RGPD en mayo 2018. Se anunciará en los Boletines de versiones correspondientes (marzo-abril-mayo)

Además, hemos creado un paquete formativo enfocado no solamente a que entiendas la nueva reglamentación; sino que entiendas, de una forma totalmente práctica y aplicable a tu negocio, cuales son las medidas que tienes que seguir para estar dentro del RGPD.

**¿ES EL SOFTWARE
DE SAGE COMPLIANCE
CON EL RGPD?
SI COMPRO VUESTRO
SOFTWARE,
¿SOY YA COMPLIANCE
CON EL RGPD?
¿QUÉ MÁS TENGO
QUE HACER?**

RGPD

Nuestro software se ha diseñado desde el inicio teniendo en cuenta la nueva reglamentación del RGPD. Una funcionalidad RGPD "llaves en mano" que contempla una gestión ágil, completa e integrada favoreciendo la productividad de nuestros clientes. Con total información respecto a los campos con datos sensibles propios de las soluciones; permitiendo ampliarlo a las adaptaciones que puedan tener algunos clientes con una configuración específica en cada caso.

El software te permitirá gobernar los datos gestionados por tu aplicación Sage bajo la nueva reglamentación del RGPD, pero además necesitarás formarte en las formaciones que Sage te proporciona para que además del producto sepas qué procedimientos debes implementar en tu negocio.

El Reglamento dice claramente que la responsabilidad del 'compliance' es sólo y exclusivamente de la empresa y no puede ser delegada a terceras partes. Esto quiere decir que es la propia empresa la que tiene que asegurar de que implementa las mejores prácticas y herramientas para gestionar la protección de datos bajo la nueva normativa.

Obviamente esto no lo podéis hacer solos, sino que necesitáis actualizaciones en vuestro software y herramientas que os permitan gobernar estos nuevos procesos.

Además, es muy recomendable que hagáis todo el plan formativo que os propone Sage, donde no sólo llegaréis a entender en profundidad las implicaciones reales de la entrada en vigor del RGPD sino que seréis capaces de identificar de forma práctica que cosas tenéis que abordar en vuestras propias empresas.

Con toda esta información, documentación, software y apoyo de Sage está en disposición de trabajar para que su negocio sea acorde al RGPD.

¿SOY COMPLIANCE CON RGPD CON LA SOLUCIÓN QUE TENGO ACTUALMENTE ¿POR QUÉ TENGO QUE ACTUALIZARME?

RGPD

Según un estudio de IDC con Microsoft el 80% de las empresas españolas contempla algún tipo de afectación e impacto en su gestión diaria por efecto del RGPD. Por ello, según los datos de ese estudio, la inversión de las empresas españolas para adaptar sus procesos y sistemas al RGPD se incrementará este año un 44% respecto al 2017.

Con las nuevas exigencias que trae el RGPD es prácticamente seguro que tendrás que revisar tus procesos de tratamiento de datos y hacer una actualización de tus herramientas software para gestionar estos nuevos procesos. Además, el RGPD exige a las empresas que sean proactivas en esto; es decir, que hagan las inversiones y los ajustes necesarios para garantizar la protección de los datos sensibles propios y de sus clientes.

Por eso desde Sage te ofrecemos una actualización de tu software para incorporar las funcionalidades específicas que te ayudarán con el RGPD. Con esta actualización, además de estar cubierto desde el inicio podrás despreocuparte porque al actualizarte, Sage se encarga de actualizar el producto continuamente acorde a las nuevas exigencias que sin duda seguirá marcando la nueva normativa y que te cubrirá el mantenimiento del software RGPD.

Capítulo 19

¿QUÉ HERRAMIENTAS OFRECÉIS PARA QUE PUEDA CUMPLIR CON EL RGPD? ¿CÓMO GESTIONO LOS CYBERATAQUES Y LA FUGA DE INFORMACIÓN DE MI EMPRESA? ¿SI ME ROBAN LOS DATOS, SOY YO RESPONSABLE FRENTE A LA NORMATIVA RGPD?

RGPD

Efectivamente la empresa/despacho es responsable ante una fuga o robo de datos, pero aportar que la empresa ha tomado medidas organizativas y técnicas adecuadas puede minimizar esa responsabilidad.

Para evitar esto y estar cubierto, debes tener un software y plan formativo como el que te ofrece Sage que te proteja desde el inicio y poder responder a estas premisas del Reglamento:

- Soy responsable y encargado del tratamiento de datos que gestiono (clientes, proveedores, empleados...) y necesito medios técnicos y organizativos que me ayuden a cumplir con mis obligaciones.
- Debo estar formado para la gestión de datos, tanto yo como mis colaboradores
- Debo evaluar mi nivel de riesgo para determinar qué acciones tengo que hacer o tener en cuenta
- Como responsable de datos debo disponer del consentimiento expreso para su uso, así como garantizar los efectos de la revocación
- Como encargado de tratamiento, debo dar garantías de aplicar medidas técnicas y organizativas adecuadas a RGPD para ser elegido por un responsable del tratamiento de datos.
- Mis datos deben estar en un entorno seguro (SQL Sage o SaaS)
- Debo garantizar un nivel de seguridad adecuado a mis riesgos: seudonimización, confidencialidad, capacidad de restauración de datos...
- Quiero saber dónde están los datos que requieren mi atención de forma fácil
- Debo asegurar que solo acceden a los datos que estoy autorizado las personas autorizadas
- Tengo que garantizar que puedo cumplir los derechos de los propietarios de los datos: Portabilidad de mis datos, olvidarlos de mí.

Sage ofrece un enfoque completo para prepararse para el cumplimiento del RGPD con formaciones, soluciones y servicios, desde la evaluación hasta su implementación completa de la

¿QUÉ HERRAMIENTAS OFRECÉIS PARA QUE PUEDA CUMPLIR CON EL RGPD? ¿CÓMO GESTIONO LOS CYBERATAQUES Y LA FUGA DE INFORMACIÓN DE MI EMPRESA? ¿SI ME ROBAN LOS DATOS, SOY YO RESPONSABLE FRENTE A LA NORMATIVA RGPD?

RGPD

(...)

funcionalidad. Nuestro enfoque cubre todas las actividades necesarias para dar soporte al RGPD: Gobierno de RGPD, comunicación y formación de todos los implicados, procesos, proteger los datos frente violaciones de seguridad y aumentar el nivel de seguridad del acceso de los usuarios.

- Software legal
- Recovery
- Bases de datos en MSSQL (la más segura del mercado)
- Autorización de acceso por usuarios
- Seguridad en las contraseñas
- Restricción de acceso a usuarios en entidades de interesados según los datos
- Restricción de acceso a usuarios en entidades según su uso (ex. No ver nómina de una empresa de conta)
- Datos en servidor seguro de Sage (para alojamiento de información o intercambio de datos)
- Kit de seguridad: Antivirus, Backup Online, Recuperación de Disco Duro y Guía de buenas practicas en seguridad.
- Microsoft Office 365, que te ayuda a cumplir con el estándar de RGPD pudiendo trabajar en la nube y a la vez dotando a tu empresa de la seguridad y del cumplimiento de la legislación de forma segura. Esta herramienta permite gestionar de forma segura los archivos que contienen ficheros con información personal, ya que según el RGPD se debe tener especial cuidado de la gestión de la información de carácter personal almacenada en ficheros desestructurados o no controlados, como puede ser un listado de clientes guardado en un disco duro no seguro o en un pendrive.

En caso de filtración de datos, la norma obliga a informar a la Administración pública en 72 horas desde que se produjo, por lo tanto, apuesta por Sage para asegurarte el mayor cumplimiento.

¿QUÉ HAGO CON LA INFORMACIÓN QUE ESTÁ FUERA DEL SOFTWARE DE CONTABILIDAD / ERP? ¿ME AYUDA SAGE CON ESTE TEMA?

RGPD

En cualquier empresa existen varios niveles o capas de información que pueden tener información sensible y, por tanto, estar obligado a gestionar y proteger conforme al nuevo reglamento del RGPD.

La primera es la información en sí contenida en tu software de gestión o contabilidad. Pero también, existen ficheros que se extraen de dichas herramientas y luego se comparten con otras personas dentro o fuera de tu organización. Por ejemplo, un informe resumen de ventas o un balance; que se calculan en base a los datos del software de gestión. Si utilizas herramientas convencionales para editarlos, almacenarlos, compartirlos muy probablemente estés incumpliendo la normativa del RGPD dado que no estás garantizando la protección de la información sensible. Para resolver este problema, Sage ofrece en sus productos Sage 50cloud y Sage 200cloud la integración con Microsoft Office 365; que no es más que la suite de office pero alojada en la nube de Microsoft y, por tanto, garantizando el cumplimiento del RGPD.

Además del software para cumplir la norma, Sage le ofrece un plan formativo para todos los involucrados en el negocio de su empresa sepa cómo tratar cada tipo de información sensible que define el reglamento. Desde la formación específica para cada tipo de empresa, a una formación para los empleados de cara saber cómo gestionar toda la información y saber cómo actuar en cada caso para no tener problemas con el RGPD.

¿QUÉ PROCEDIMIENTOS ESTÁN CUBIERTOS Y CUÁLES NO?

RGPD

Procedimientos obligatorios en el nuevo RGPD en el tratamiento de los datos personales:

- Informar de la Finalidad y Uso de los datos personales a los interesados
- Obtener el Consentimiento de una forma explícita (de forma libre, específica e inequívoca, mediante declaración o clara acción informativa)
- Posibilidad de limitar el tiempo del consentimiento del uso de los datos personales
- Obtener y trasladar el Consentimiento de Cesión de datos a Terceros (asesorías, empresas de telemarketing, empresas de publicidad, etc.)
- Existencia de un Delegado de Protección de datos (DPD) dentro de la organización para empresas de gran envergadura (+250 empleados)
- Recoger la revocación del Consentimiento de la autorización del tratamiento de los datos
- Guardar información de datos personales sólo el tiempo autorizado o mientras existe obligación legal
- Controlar las salidas de información de datos personales en comunicaciones, mailing, exportaciones, etc.

Ejemplos de procedimientos no válidos para el RGPD:

- Envío de documentación con datos sensibles por email
- Guarda de documentos con información sensible no estructurada en un pendrive o disco duro.

**¿POR QUÉ NO ME
DAIS ESTO DENTRO
DE MI CONTRATO DE
MANTENIMIENTO
ACTUAL? ¿VOY
A NECESITAR
COMPRARLO
CADA VEZ QUE
HAYA UN CAMBIO
NORMATIVO?**

RGPD

El nuevo reglamento RGPD exige que las empresas revisen todos sus procesos de protección de datos; esto implica no solamente el software de gestión y contabilidad sino cualquier todo que gestione información sensible.

Si embargo, es cierto que los ERP y software de gestión y contabilidad son quizás los más susceptibles de gestionar este tipo de información sensible. Por ello, Sage ha desarrollado una funcionalidad RGPD específica que amplía y mejora la funcionalidad actual de su versión para facilitar el cumplimiento de la normativa. De hecho, los nuevos productos Sage 50cloud, Sage 200cloud y SD4L ya han sido diseñados bajo las premisas del RGPD, por lo que le recomendamos encarecidamente hacer una migración a estos productos.

**¿POR QUÉ DEBERÍA
CONTRATAR LOS
SERVICIOS DE RGPD A
SAGE?
¿EN QUÉ SE DIFERENCIA
CON OTRAS OFERTAS
QUE HE RECIBIDO?
NO LO NECESITO,
YA HE EXTERNALIZADO
ESTE SERVICIO A UN
DESPACHO PROFESIONAL/
EMPRESA ESPECIALIZADA
PARA EVITAR PROBLEMAS**

RGPD

Aunque hayas externalizado el servicio, tú como empresa tienes que cumplir la normativa desde el inicio. En el día a día de tu negocio, tanto empleados como gerentes estáis trabajando con datos sensibles al RGPD todos los días y realizáis procedimientos que podrían estar afectados por la nueva normativa. El RGPD te afecta en la forma de desarrollar tu negocio y tienes que cambiar la forma y procedimientos de muchos de los procesos que haces ahora. Si esto lo desconoces, estarás incumpliendo continuamente la normativa.

Una cosa es externalizar parte del servicio (control de la información, etc) y otra cosa es que tú como empresa debas trabajar diariamente conforme el nuevo RGPD.

Para valorar tu situación frente a las principales obligaciones del RGPD, deberíamos fijarte bien en cuestiones como:

1. Legitimación: ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?
2. Información y derechos: La información que se proporciona a los interesados, ¿contiene todos los elementos que prevé el RGPD? ¿Tiene establecidos procedimientos que le permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD?
3. Medidas de responsabilidad proactiva: ¿Ha hecho una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos? ¿Ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas? ¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos? ¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?

**¿POR QUÉ DEBERÍA
CONTRATAR LOS
SERVICIOS DE RGPD A
SAGE?
¿EN QUÉ SE DIFERENCIA
CON OTRAS OFERTAS
QUE HE RECIBIDO?
NO LO NECESITO,
YA HE EXTERNALIZADO
ESTE SERVICIO A UN
DESPACHO PROFESIONAL/
EMPRESA ESPECIALIZADA
PARA EVITAR PROBLEMAS**

RGPD

(...)

El Reglamento exige medidas organizativas en el negocio y formas de actuación de cada una de las personas que manejan datos sensibles en el mismo, por ello, Sage ante la relevancia de esta normativa, para asegurar su cumplimiento y para ayudar a cada cliente a adecuar todo su negocio a este reglamento le ofrecemos el Plan normativo para que tanto el negocio como sus colaboradores y clientes, esté preparado para la nueva ley con tiempo suficiente para prepararse para la norma. Sage le ofrece un plan formativo para todos los involucrados en el negocio de su empresa sepa cómo tratar cada tipo de información sensible que define el reglamento. Desde la formación específica para cada tipo de empresa, a una formación para los empleados de cara a cumplir exhaustivamente cada uno de los requerimientos del nuevo RGPD

Así mismo, Sage se compromete a mantenerte siempre actualizado según vayan saliendo nuevas exigencias dentro de esta norma que sabemos que estará viva, y así te desprocurarás de estar pendiente si cumples o no, cedes la necesidad de estar siempre actualizado a Sage.

No se engañe, si hay alguna fuga de seguridad, una demanda o una inspección, la responsabilidad es suya, independientemente de si ha "externalizado el servicio".

sage