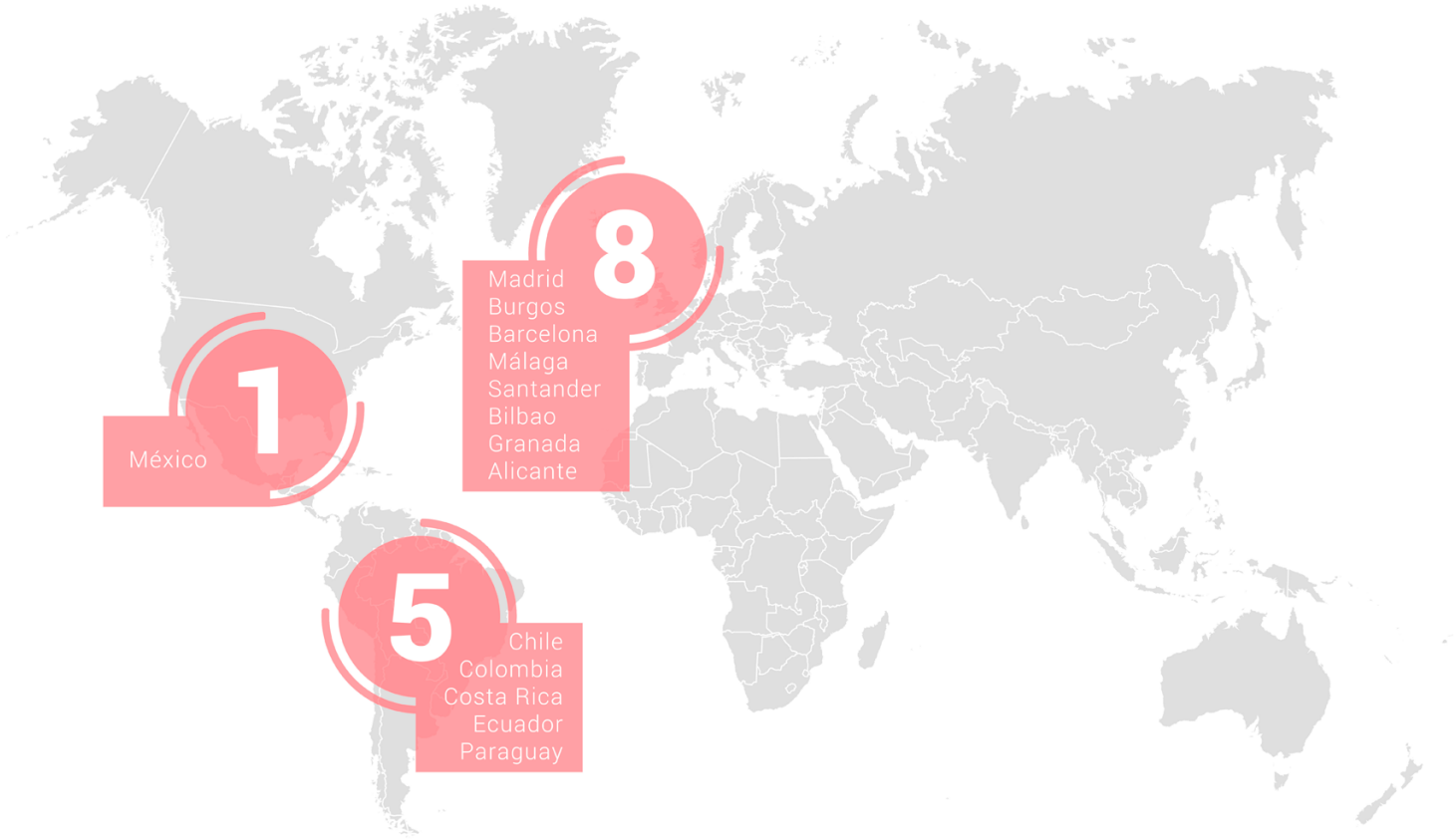
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Implicaciones del Reglamento General de Protección de Datos



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicada el 02/12/2016

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD). Aunque no comenzará a aplicarse hasta dos años después, es importante que las organizaciones vayan adaptando sus procesos, ya que la nueva normativa supone una gestión distinta de la que se viene empleando.

La Agencia Española de Protección de Datos (AEPD), en su faceta preventiva, quiere fomentar que las entidades puedan conocer las posibles dificultades en su aplicación para tomar medidas que permitan solventarlas. A continuación se analizan algunas de las implicaciones prácticas que conviene que las entidades conozcan para afrontar el momento en el que el Reglamento sea aplicable. La AEPD está comprometida con conseguir que la aplicación del RGPD se produzca con pleno respeto a sus disposiciones y, al mismo tiempo, con ofrecer la mayor flexibilidad posible.

1. Consentimiento

El Reglamento requiere que las personas cuyos datos se tratan presten su consentimiento mediante una manifestación inequívoca o una clara acción afirmativa. Esto excluye la utilización del llamado consentimiento tácito, que actualmente permite la normativa española. Los consentimientos obtenidos con anterioridad a la fecha de aplicación del RGPD sólo seguirán siendo válidos como base de tratamiento si se obtuvieron respetando los criterios fijados por el propio Reglamento.

La Agencia aconseja que las organizaciones que en estos momentos utilizan el llamado consentimiento tácito como base para los tratamientos comiencen tanto a revisar los consentimientos ya obtenidos para adecuarlos al Reglamento como a utilizar mecanismos acordes con la nueva legislación. A partir de mayo de 2018, sólo tendrán legitimación suficiente los tratamientos basados en el consentimiento inequívoco, con independencia de cuándo se haya obtenido ese consentimiento.

2. Información

En materia de información el RGPD incluye cuestiones adicionales que actualmente no son requeridas por la normativa española. Cabe plantearse, por tanto, qué va a suceder con todas las cláusulas informativas utilizadas con anterioridad a mayo de 2018 una vez que el Reglamento sea de aplicación.

Este periodo transitorio debería ser utilizado por las organizaciones para realizar una adaptación progresiva por varias vías. Por una parte, muchas organizaciones pueden proporcionar esa información adicional sin costes o esfuerzos excesivos utilizando para ello sus páginas web o aprovechando los canales de comunicación regulares que puedan mantener con sus clientes. Estas buenas prácticas contribuirían a reducir el número de casos en que las cláusulas informativas presenten carencias cuando el Reglamento sea de aplicación.

Al mismo tiempo, es aconsejable que las organizaciones adapten sus políticas informativas a lo dispuesto por el Reglamento. Hay algunas cuestiones donde esa información dependerá de la adopción de otras decisiones, como puede ser el proporcionar los datos del Delegado de Protección de Datos. Esos datos no podrán trasladarse a los interesados hasta que ese Delegado no sea designado en los casos en que el Reglamento lo hace obligatorio o cuando las organizaciones decidan voluntariamente nombrarlo pero otros elementos sí pueden ya anticiparse y, en la medida de lo posible, incorporarse sin dilación a las informaciones que se proporcionan a los interesados.

3. Evaluaciones de impacto sobre la protección de datos

La realización de Evaluaciones de Impacto sobre la protección de datos ?aplicables de forma obligatoria en ciertos tratamientos- tiene carácter previo a la puesta en marcha de los mismos y tiene como objetivo minimizar los riesgos que un tratamiento de datos plantea para los ciudadanos. Por ello, posiblemente no sería acorde con el espíritu del Reglamento exigir que todo tratamiento que pueda potencialmente suponer un alto riesgo para los derechos de los interesados deba ser objeto de una Evaluación de Impacto pese a haber comenzado antes de que resulte aplicable.

Sin embargo, en la medida en que esos tratamientos incorporen, a partir de mayo de 2018, nuevos datos, debe entenderse que, pese a que el tratamiento siga siendo el mismo, se estaría aplicando a nuevos interesados cuyos derechos y libertades podrían estar en riesgo a partir de la fecha en que sus datos comienzan a ser tratados. Por ello, en esos casos sí sería necesario que se llevara a cabo una EIPD en los supuestos a los que se refiere el RGPD.

En los demás casos en que las evaluaciones puedan ser obligatorias, la Agencia considera que no debería esperarse a la fecha de aplicación del Reglamento para comenzar a utilizar esta herramienta, ya que requiere de preparación, elección de la metodología adecuada, identificación de los equipos de trabajo y otra serie de condiciones que no pueden improvisarse.

Comenzar a incorporar este sistema a la actuación de las organizaciones no sólo va a permitirles estar en mejores condiciones en el momento en que resulte obligatorio para algunas de ellas, sino que también les permitirá asegurar el cumplimiento no ya del futuro Reglamento, sino incluso de la actual normativa.

4. Certificación

El Reglamento concede una atención especial a la implantación de esquemas de certificación y abre diversas posibilidades para su gestión. Las certificaciones pueden ser otorgadas por las Autoridades de protección de datos, tanto individual como colectivamente desde el Comité Europeo, o por entidades debidamente acreditadas. Al mismo tiempo, en el caso de optarse por esta última alternativa, la acreditación pueden llevarla a cabo las propias Autoridades o encargarlo a las entidades de acreditación previstas en la normativa europea sobre normalización y certificación. En todo caso, en la elaboración de los criterios tanto para acreditar entidades como para certificar a las organizaciones tienen diferentes grados de participación las autoridades de supervisión y el Comité Europeo.

La AEPD entiende que, de entre estas posibilidades, la que mejor responderá a las necesidades de las entidades al tiempo que es compatible con la configuración y posibilidades de actuación de la Agencia es la de encomendar la certificación a entidades especializadas debidamente acreditadas y dejar que se ocupe de la acreditación de éstas la Entidad Nacional de Acreditación (ENAC), contando para ello con la participación de la Agencia.

5. Delegados de protección de datos. Certificación

El Reglamento requiere que los Delegados de Protección de Datos (DPD) sean nombrados en función de sus cualificaciones profesionales, en especial su conocimiento en materia de protección de datos, y su capacidad para el desempeño de sus funciones. Sin embargo, no establece específicamente cuáles han de ser esas cualificaciones profesionales ni tampoco el modo en que podrán demostrarse ante las organizaciones que deban incorporar esta figura. De hecho, el Reglamento indica en uno de sus considerandos que la valoración de estas aptitudes y conocimientos

deberá realizarse no tanto en función de criterios externos como de las necesidades de los tratamientos concretos que cada organización lleve a cabo.

La Agencia considera que no es oportuno establecer un sistema de certificación de Delegados de Protección de Datos que opere como requisito para el acceso a la profesión.

En este momento, ya existe una oferta de certificaciones y titulaciones que respaldan conocimientos, experiencia o práctica en el ámbito de la protección de datos. Esas titulaciones están llamadas a jugar un papel relevante en el desarrollo de las profesiones relacionadas con la protección de datos en la medida en que pueden servir como un elemento más, aunque no sea necesariamente único, para que la organización que tiene que designar un DPD pueda tener constancia de la formación o cualificaciones de los posibles candidatos.

Para que la oferta de certificaciones y titulaciones funcione de manera rigurosa es necesario que estas reúnan unos requisitos que permitan que las entidades que los reciban puedan tener un razonable grado de certeza sobre lo que reflejan.

La Agencia está valorando la posibilidad de promover la aplicación de la acreditación de entidades de certificación de profesionales con arreglo a estándares ya establecidos. Esta acreditación, que llevaría a cabo la Entidad Nacional de Acreditación (ENAC) de acuerdo con lo previsto en esos estándares y con las peculiaridades propias del sector, serviría para constatar que la entidad que expide los títulos, certificados o certificaciones lo hace con arreglo a unos determinados procedimientos y requisitos. La acreditación no se pronuncia sobre la calidad de los contenidos de la formación o de los aspectos que se certifican.

El hecho de que algunas entidades se acrediten no implicará necesariamente que otras que no lo hagan no apliquen los mismos criterios ni tampoco que la posesión de la titulación o certificación sea la única vía para acceder a un puesto de Delegado de Protección de Datos.

La Agencia considera que estas cuestiones tendrían un carácter instrumental orientado a ofrecer apoyo a las organizaciones a la hora de designar a un DPD. No obstante, en ningún caso excluyen que profesionales con formaciones procedentes de centros no acreditados o sin una formación específica pero con experiencia profesional puedan desempeñar las funciones de Delegado si su currículo muestra que reúnen los requisitos de conocimiento y cualidades

profesionales que el Reglamento establece.

6. Relación entre responsables y encargados

El Reglamento describe un contenido mínimo de los contratos de encargo de tratamiento que excede las previsiones contempladas en la Directiva. En el caso español, la LOPD ya contempla la inclusión de algunos de esos contenidos en los contratos, aunque hay diferencias entre esta y en RGPD en relación a los requisitos fijados.

El contrato es el documento que determina las obligaciones de las partes ante la prestación del servicio de encargo que se acuerda. Por ello, debe respetar en todo caso el contenido fijado por el Reglamento ya que, en caso contrario, no se estarían trasladando a los encargados las obligaciones que el Reglamento específicamente prevé.

Este momento de transición entre la entrada en vigor y la aplicación del RGPD debería aprovecharse para llevar a cabo dos acciones paralelas. En primer lugar, para abordar la revisión de los contratos ya existentes y que se refieran a encargos con vocación de prolongarse en el tiempo, de forma que en mayo de 2018 sean compatibles con las disposiciones del Reglamento. En segundo lugar, para comenzar a incluir en las nuevas cláusulas contractuales todos los elementos que el Reglamento considera necesarios.

La Agencia, en colaboración con las Agencias autonómicas, está trabajando en la preparación de unas recomendaciones para los contratos de encargo. No se trata de los modelos de contrato a que se refiere el Reglamento debido a que esos modelos requieren de aprobación por parte del Comité Europeo de Protección de Datos -que aún no se ha establecido-, si bien tienen el objetivo de servir de orientación en esta primera etapa para que las organizaciones respondan a los nuevos requerimientos.

7. Herramientas para pymes y herramientas sectoriales

La Agencia está trabajando en la preparación de herramientas que ayuden a responsables y encargados al entendimiento y cumplimiento del Reglamento. Entre ellas, hay que destacar un recurso online orientado a las pymes que realicen tratamientos de bajo o muy bajo riesgo, de forma que puedan constatar de una manera sencilla que se encuentran en esa situación y, a la vez, disponer de una lista de las medidas que tienen que implantar en función de ese bajo nivel de riesgo.

Está previsto que este recurso se complemente con otros más avanzados, orientados a las pymes que desarrollan tratamientos que conllevan un nivel de riesgo algo mayor como consecuencia de alguna circunstancia concreta -como puede ser el manejo de datos sensibles- y que incluirá un apartado dedicado a las medidas de seguridad que deben implantarse.

La AEPD está trabajando junto a las Agencias autonómicas en cláusulas informativas adaptadas al nuevo Reglamento para sectores o tratamientos diferenciados. Así, está previsto ofrecer una serie de recomendaciones o criterios para ayudar a reflejar los distintos puntos que el Reglamento exige en la información.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com