



Bruselas, 24.1.2018
COM(2018) 43 final

**COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL
CONSEJO**

**Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la
aplicación directa del Reglamento general de protección de datos a partir del 25 de
mayo de 2018**

Comunicación de la Comisión al Parlamento Europeo y al Consejo

Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018

Introducción

El 6 de abril de 2016, la Unión Europea (UE) acordó una importante reforma de su marco en materia de protección de datos, mediante la adopción del paquete legislativo de reforma de la protección de datos, que incluye el Reglamento general de protección de datos (RGPD)¹, el cual sustituye a la Directiva 95/46/CE, vigente desde hacía veinte años² («Directiva sobre protección de datos»), y a la Directiva sobre la cooperación policial³. El 25 de mayo de 2018, el nuevo instrumento de protección de datos a escala de la UE, el Reglamento general de protección de datos (en lo sucesivo, «el Reglamento»), será directamente aplicable, dos años después de su adopción y entrada en vigor⁴.

El nuevo Reglamento reforzará la protección del derecho de las personas a la protección de los datos personales, reflejando la naturaleza de la protección de datos como derecho fundamental de la Unión Europea⁵.

Al establecer un conjunto único de normas directamente aplicables en los ordenamientos jurídicos de los Estados miembros, garantizará la libre circulación de los datos de carácter personal entre los Estados miembros de la UE y reforzará la confianza y la seguridad de los consumidores, dos elementos imprescindibles para un verdadero mercado único digital. De esta forma, el Reglamento creará nuevas oportunidades para negocios y empresas, especialmente los más pequeños, haciendo también que las normas resulten más claras para las transferencias internacionales de datos.

Aunque el nuevo marco de protección de datos se basa en la legislación vigente, tendrá una gran repercusión en numerosos ámbitos y requerirá ajustes significativos en determinados aspectos. Por este motivo, en el Reglamento se estableció un periodo transitorio de dos años, hasta el 25 de mayo de 2018, a fin de dar a los Estados miembros y a las partes interesadas tiempo para prepararse plenamente para el nuevo marco jurídico.

¹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016).

² Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995).

³ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016).

⁴ El Reglamento está en vigor desde el 24 de mayo de 2016 y se aplicará a partir del 25 de mayo de 2018.

⁵ Artículo 8 de la Carta de los Derechos Fundamentales de la UE y artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

A lo largo de los dos últimos años, todas las partes interesadas, desde las administraciones nacionales y las autoridades nacionales de protección de datos hasta los responsables y los encargados del tratamiento de los datos, han llevado a cabo una serie de actividades para garantizar que la importancia y el alcance de los cambios introducidos por el nuevo régimen de protección de datos se entienden debidamente y que todos los actores están listos para su aplicación. Dado que el plazo del 25 de mayo se acerca, la Comisión considera que es necesario hacer balance de estos trabajos y examinar cualquier medida adicional que pueda ser útil para garantizar que existen todos los elementos para el éxito de la aplicación efectiva del nuevo marco⁶.

La presente Comunicación:

- recapitula las principales innovaciones y oportunidades que ofrece la nueva legislación de la UE en materia de protección de datos;
- evalúa los trabajos preparatorios realizados hasta la fecha a nivel de la UE;
- resume todo aquello que la Comisión Europea, las autoridades nacionales de protección de datos y las administraciones nacionales tienen aún pendiente para llevar a buen término la preparación;
- establece las medidas que la Comisión tiene previsto adoptar en los próximos meses.

Por otra parte, de manera paralela a la adopción de la presente Comunicación, la Comisión pone en marcha una serie de herramientas en línea para ayudar a las partes interesadas a prepararse para la aplicación del Reglamento y, con la ayuda de las oficinas de representación, una campaña de información en todos los Estados miembros.

1. EL NUEVO MARCO DE PROTECCIÓN DE DATOS DE LA UE: MAYOR PROTECCIÓN Y NUEVAS OPORTUNIDADES

El Reglamento sigue el enfoque de la Directiva sobre protección de datos, aunque, basándose en los veinte años de legislación de la UE en materia de protección de datos y en la jurisprudencia pertinente, aclara y moderniza las normas al respecto. Introduce una serie de elementos nuevos que refuerzan la protección de los derechos de la persona y abren oportunidades a las empresas y los negocios, en concreto:

- **Un marco jurídico armonizado que conduce a una aplicación uniforme de las normas en beneficio del mercado único digital de la UE.** Esto significa un conjunto único de normas para los ciudadanos y las empresas. De este modo se tratará la actual situación, en la que los Estados miembros de la UE han aplicado las normas de la Directiva de distinta manera. Para garantizar una aplicación uniforme y coherente en todos los Estados miembros, se introduce un mecanismo de ventanilla única.
- **Igualdad de condiciones para todas las empresas que operan en el mercado de la UE.** El Reglamento exige que las empresas con sede fuera de la UE apliquen las mismas normas que las empresas establecidas en su territorio si ofrecen bienes y servicios relacionados con datos de carácter personal o si realizan un seguimiento del comportamiento de las personas en la Unión. Las empresas que operan desde fuera de la UE y realizan actividades en el mercado único deben, en determinadas circunstancias,

⁶ https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_es.pdf.

designar a un representante en la UE al que los ciudadanos y las autoridades puedan dirigirse además de a la empresa con sede en el extranjero o en lugar de a ella.

- **Los principios de protección de datos desde el diseño y por defecto**, creando incentivos para la adopción de soluciones innovadoras que aborden las cuestiones relativas a la protección de los datos desde el principio.
- **Fortalecimiento de los derechos de las personas**: el Reglamento introduce nuevos requisitos de transparencia; derechos reforzados de información, acceso y eliminación («derecho al olvido»); el silencio o la falta de actividad dejarán de considerarse como un consentimiento válido, ya que se requiere una clara acción afirmativa para expresar dicho consentimiento; y la protección de los niños en línea.
- **Mayor control sobre los datos personales para los particulares**. El Reglamento establece un **nuevo derecho a la portabilidad de los datos** que permite a los ciudadanos solicitar que una empresa u organización le devuelva los datos personales que le facilitó por consentimiento o contrato; también permitirá que dichos datos personales se transmitan directamente a otra empresa u organización, cuando sea técnicamente posible. Dado que permite la transmisión directa de datos personales de una empresa u organización a otra, este derecho también apoyará la libre circulación de los datos personales en la UE, evitará la retención de datos personales, y fomentará la competencia entre empresas. Facilitar a los ciudadanos el cambio entre distintos proveedores impulsará el desarrollo de nuevos servicios en el contexto de la estrategia del mercado único digital.
- **Mayor protección contra las violaciones de la seguridad de los datos**. El Reglamento establece un conjunto completo de normas en materia de violación de la seguridad de los datos personales. Define claramente qué es una «violación de la seguridad los datos personales», introduce la obligación de notificación a la autoridad de control, a más tardar, en un plazo de 72 horas cuando sea probable que la violación de la seguridad de los datos constituya un riesgo para los derechos y las libertades de la persona. En determinadas circunstancias, obliga a informar a la persona cuyos datos se ven afectados por la violación. Esto refuerza considerablemente la protección en comparación con la actual situación en la UE, en la que solo los proveedores de servicios de comunicaciones electrónicas, los operadores de servicios básicos y los proveedores de servicios digitales están obligados a notificar las violaciones de la seguridad de datos personales en el marco de la Directiva sobre la privacidad y las comunicaciones electrónicas⁷ y la Directiva sobre la seguridad de las redes y sistemas de información (Directiva SRI)⁸, respectivamente.

⁷ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, pp. 37-47). Según el artículo 95 del Reglamento general de protección de datos, dicho Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE. Esto significa, por ejemplo, que las entidades a las que se aplica la Directiva sobre la privacidad y las comunicaciones electrónicas están sujetas a la obligación establecida en dicha Directiva de notificar toda violación de la seguridad de los datos personales en la medida en que esa violación se refiera a un servicio que esté regulado por lo dispuesto en esa Directiva. En ese aspecto, el RGPD no les impone obligaciones adicionales.

⁸ Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, pp. 1-30). Las entidades incluidas en el ámbito de aplicación de la Directiva

- **El Reglamento concede a todas las autoridades de protección de datos competencias para imponer multas a los responsables y encargados del tratamiento.** Actualmente no todos ellos disponen de esta facultad. Esto propiciará una mejor aplicación de las normas. Las multas pueden ascender hasta los 20 millones EUR o, en el caso de una empresa, hasta el 4 % de su volumen de negocios anual a nivel mundial.
- **Mayor flexibilidad para los responsables y los encargados del tratamiento que procesan datos personales gracias a unas disposiciones inequívocas sobre la responsabilidad (principio de responsabilidad proactiva).** El Reglamento pasa de un sistema de notificación al principio de responsabilidad proactiva. Este último se aplica a través de obligaciones graduales en función de los riesgos (por ejemplo, la presencia de un delegado de protección de datos o la obligación de realizar evaluaciones de impacto relativas a la protección de datos). Se introduce un nuevo instrumento para ayudar a evaluar el riesgo antes de que se inicie el tratamiento: la evaluación de impacto relativa a la protección de datos. Esta debe realizarse cada vez que sea probable que el tratamiento dé lugar a un riesgo elevado para los derechos y libertades de las personas. Con arreglo al Reglamento, se mencionan específicamente tres situaciones de este tipo: cuando una empresa evalúa de forma sistemática y en profundidad aspectos personales de un individuo (incluida la elaboración de perfiles), cuando procesa datos sensibles a gran escala o cuando realiza un control sistemático de zonas públicas a gran escala. Las autoridades nacionales de protección de datos deberán publicar las listas de los casos que requieran una evaluación de impacto relativa a la protección de datos⁹.
- **Mayor claridad en cuanto a las obligaciones de los encargados y de los responsables del tratamiento a la hora de elegir a un encargado.**
- **Un sistema de gobernanza moderno para garantizar que las normas se aplican de forma más coherente y firme.** Esto incluye la armonización de las competencias de las autoridades de protección de los datos, también por lo que respecta a las multas, y nuevos mecanismos para que estas autoridades cooperen en una red.
- **La protección de los datos personales que el Reglamento garantiza se desplaza junto con los datos al exterior de la UE, asegurando un elevado nivel de protección¹⁰.** Si bien la arquitectura de las normas sobre transferencias internacionales recogida en el Reglamento sigue siendo fundamentalmente la misma que la de la Directiva de 1995, la reforma aclara y simplifica su utilización e introduce nuevas herramientas para las transferencias. Por lo que se refiere a las decisiones sobre la adecuación de la protección, el Reglamento introduce un catálogo preciso y detallado de los elementos que la Comisión debe tener en cuenta a la hora de evaluar si un sistema extranjero protege adecuadamente los datos de carácter personal. Además, el Reglamento formaliza y amplía el número de instrumentos de transferencia alternativos como, por ejemplo, cláusulas contractuales tipo y normas corporativas vinculantes.

SRI deben notificar cualquier incidente que tenga una repercusión importante o sustancial en la prestación de algunos de sus servicios. La notificación de incidentes con arreglo a la Directiva SRI se entiende sin perjuicio de la notificación de la violación de la seguridad en virtud del Reglamento.

⁹ Artículo 35 del Reglamento.

¹⁰ Comunicación de la Comisión «Intercambio y protección de los datos personales en un mundo globalizado», COM(2017) 7 final.

El Reglamento revisado para las instituciones, órganos y organismos de la UE¹¹ y el Reglamento sobre la privacidad y las comunicaciones electrónicas¹², que se encuentran actualmente en fase de negociación, una vez adoptados, garantizarán que la UE esté dotada de un conjunto de normas de protección de datos¹³ sólido y completo.

2. TRABAJOS PREPARATORIOS REALIZADOS HASTA LA FECHA A NIVEL DE LA UE

El éxito de la aplicación del Reglamento requiere la cooperación entre todas las partes implicadas en la protección de los datos: los Estados miembros, incluidas administraciones públicas, autoridades nacionales de protección de datos, empresas, organizaciones que tratan datos personales y particulares, así como la Comisión.

2.1. Acciones por parte de la Comisión Europea

Poco después de la entrada en vigor del Reglamento a mediados de 2016, la Comisión inició el trabajo con las autoridades de los Estados miembros, las autoridades de protección de datos y las partes interesadas para preparar la aplicación del Reglamento y proporcionar apoyo y asesoramiento.

a) Apoyo a los Estados miembros y sus autoridades

La Comisión ha colaborado estrechamente con los Estados miembros para apoyar su trabajo durante el período transitorio, con el fin de garantizar el nivel más elevado posible de coherencia. A tal fin, la Comisión ha creado un grupo de expertos encargado de acompañar a los Estados miembros en su labor de preparación para el Reglamento. El grupo, que se ha reunido ya en trece ocasiones, actúa como foro en el que los Estados miembros pueden compartir sus experiencias y conocimientos¹⁴. La Comisión ha participado también en reuniones bilaterales con las autoridades de los Estados miembros para debatir cuestiones que surgen a nivel nacional.

b) Apoyo a las distintas autoridades de protección de datos y a la creación del Comité Europeo de Protección de Datos

¹¹ Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión 1247/2002/CE, COM(2017) 8 final.

¹² Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM(2017) 10 final.

¹³ Hasta la adopción y entrada en vigor del Reglamento sobre la privacidad y las comunicaciones, se aplicará la Directiva 2002/58/CE como *lex specialis* con respecto al Reglamento.

¹⁴ Para consultar una lista completa de las reuniones, las órdenes del día, el resumen de los debates y una visión general de la situación de la legislación en los distintos Estados miembros, véase http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail_groupDetail&groupID=3461&Lang=ES.

La Comisión ha apoyado activamente la labor del Grupo de Trabajo del artículo 29, también con vistas a facilitar la transición al Comité Europeo de Protección de Datos¹⁵.

c) Divulgación internacional

El Reglamento reforzará aún más la capacidad de la UE para promover activamente sus valores relativos a la protección de datos y facilitar los flujos de datos transfronterizos, fomentando la convergencia de los sistemas jurídicos a nivel mundial¹⁶. Las normas de protección de datos de la UE gozan de un reconocimiento cada vez mayor a escala internacional, ya que los niveles de protección de datos que establecen figuran entre los más elevados del mundo. El Convenio n.º 108 del Consejo de Europa, el único instrumento multilateral jurídicamente vinculante en el ámbito de la protección de los datos de carácter personal, también se está modernizando. La Comisión está trabajando para que refleje los mismos principios que los recogidos en las nuevas normas sobre protección de datos de la UE y que, de este modo, ayude a establecer un conjunto uniforme de normas de elevado nivel de protección de datos. La Comisión promoverá activamente la rápida adopción del texto modernizado del Convenio, con miras a que la UE sea Parte¹⁷ en él. La Comisión anima a los países no pertenecientes a la Unión a ratificar el Convenio n.º 108 del Consejo de Europa y su Protocolo Adicional.

Además, diversos países y organizaciones regionales fuera de la UE, desde los países geográficamente más cercanos hasta Asia, América Latina y África, están adoptando nueva legislación sobre protección de datos o actualizando la ya existente para aprovechar las oportunidades que ofrece la economía digital mundial y responder a la creciente demanda de una seguridad de los datos y una protección de la privacidad mayores. Aunque los países difieren en su enfoque y su nivel de desarrollo legislativo, hay indicios de que el Reglamento tiene cada vez más peso como punto de referencia y fuente de inspiración¹⁸.

En este contexto, la Comisión continúa su labor de divulgación internacional en consonancia con su Comunicación de enero de 2017¹⁹, trabajando activamente con los principales socios comerciales, en especial del Asia oriental y sudoriental y de América Latina, para estudiar la posibilidad de adoptar decisiones sobre adecuación²⁰.

En concreto, la Comisión está trabajando con Japón para llegar a una decisión simultánea sobre un adecuado nivel de protección por ambas partes para comienzos de 2018, según lo anunciado por el presidente Juncker y el primer ministro Abe en su declaración conjunta del 6

¹⁵ Por ejemplo, la Comisión brindará al Comité Europeo de Protección de Datos la posibilidad de utilizar el Sistema de Información del Mercado Interior (IMI) para la comunicación entre sus miembros.

¹⁶ Documento de reflexión sobre el encauzamiento de la globalización COM(2017) 240.

¹⁷ Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108) y Protocolo Adicional de 2001 del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y los flujos transfronterizos de datos (STCE n.º 181). El Convenio, cuya firma no está supeditada a la pertenencia al Consejo de Europa, ya ha sido ratificado por 51 países (entre ellos, Uruguay, Mauricio, Senegal y Túnez).

¹⁸ http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf. Véanse, por ejemplo, los «Estándares de protección de datos personales para los Estados Iberoamericanos», http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf.

¹⁹ COMP(2017) 7.

²⁰ COM(2017) 7 *ibid.* pp. 10-11.

de julio de 2017²¹. Se han iniciado también conversaciones con Corea del Sur, con vistas a una posible decisión de adecuación. La adopción de una decisión sobre adecuación aseguraría la libre circulación de los flujos de datos con los terceros países de los que se trate, garantizando al mismo tiempo que se aplica un alto nivel de protección cuando se transfieran datos de carácter personal desde la UE a estos países.

Al mismo tiempo, la Comisión está trabajando con las partes interesadas para aprovechar todo el potencial que ofrece el conjunto de herramientas del RGPD para las transferencias internacionales mediante el desarrollo de mecanismos de transferencia alternativos adaptados a las necesidades específicas de industrias u operadores²² concretos.

d) Colaboración con las partes interesadas

La Comisión ha organizado una serie de eventos para llegar a las partes interesadas²³. Para el primer trimestre de 2018 está previsto un nuevo taller dirigido a los consumidores. También han tenido lugar debates sectoriales específicos en áreas como la investigación y los servicios financieros.

La Comisión ha creado también un grupo multilateral sobre el Reglamento, compuesto por representantes de la sociedad civil y del sector empresarial, representantes del mundo académico y profesionales. Este grupo asesorará a la Comisión, en concreto sobre el modo de lograr un nivel adecuado de sensibilización sobre el Reglamento en las partes interesadas²⁴.

Por último, la Comisión Europea, a través de su programa marco de investigación e innovación, Iniciativa Horizonte 2020²⁵, ha financiado acciones para desarrollar herramientas que apoyen la aplicación efectiva de las normas en virtud del Reglamento relativas al consentimiento y sobre los métodos de protección de la privacidad de los análisis de datos, tales como la informática compartida y el cifrado homomórfico.

2.2. Acciones del Grupo de trabajo del artículo 29 / Comité Europeo de Protección de Datos

El Grupo de trabajo del artículo 29, que reúne a todas las autoridades nacionales de protección de datos, incluido el Supervisor Europeo de Protección de Datos, desempeña un papel fundamental en la preparación de la aplicación del Reglamento mediante la formulación de orientaciones para las empresas y otras partes interesadas. Como encargadas de velar por el cumplimiento del Reglamento y contacto directo para las partes interesadas, las autoridades nacionales de protección de datos son las mejor situadas para proporcionar mayor seguridad jurídica en relación con la interpretación del Reglamento.

²¹ http://europa.eu/rapid/press-release_STATEMENT-17-5182_es.htm.

²² COM(2017) 7 *ibid.* pp. 10-11.

²³ Dos talleres con el sector, en julio de 2016 y abril de 2017, dos mesas redondas empresariales, en diciembre de 2016 y mayo de 2017, un taller sobre los datos sanitarios, en octubre de 2017, y un taller con representantes de las pymes, en noviembre de 2017.

²⁴ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537>

²⁵ <https://ec.europa.eu/programmes/horizon2020/h2020-sections>

Orientaciones/documentos de trabajo del Grupo de trabajo del artículo 29 con vistas al comienzo de la aplicación del Reglamento ²⁶	
Derecho a la portabilidad de los datos	Adoptados el 4 y el 5 de abril de 2017
Delegados de protección de datos	
Nombramiento de la autoridad de control principal	
Evaluación de impacto relativa a la protección de datos	Adoptado el 3 y el 4 de octubre de 2017
Multas administrativas	Adoptado el 3 y el 4 de octubre de 2017
Elaboración de perfiles	Trabajo en curso
Violación de la seguridad de los datos	Trabajo en curso
Consentimiento	Trabajo en curso
Transparencia	Trabajo en curso
Certificación y acreditación	Trabajo en curso
Referencias sobre adecuación	Trabajo en curso
Normas corporativas vinculantes para los responsables del tratamiento	Trabajo en curso
Normas corporativas vinculantes para los encargados	Trabajo en curso

El Grupo de trabajo del artículo 29 está trabajando para actualizar las opiniones existentes, en concreto sobre las herramientas para la transferencia de datos a países no pertenecientes a la UE.

Ya que es fundamental que los operadores dispongan de un conjunto de orientaciones único y coherente, las directrices actuales a nivel nacional deben derogarse o adaptarse a las adoptadas por el Grupo de trabajo del artículo 29 o el Comité Europeo de Protección de Datos sobre el mismo tema.

La Comisión concede gran importancia al hecho de que esas orientaciones sean objeto de consulta pública antes de su finalización. Es esencial que la aportación de las partes interesadas en este proceso sea lo más precisa y concreta posible, ya que esto ayudará a identificar las mejores prácticas y dará a conocer al Grupo de trabajo del artículo 29 especificidades sectoriales y de la industria. La responsabilidad final de esas orientaciones sigue siendo del Grupo de trabajo del artículo 29 y del futuro Comité Europeo de Protección de Datos y las autoridades de protección de datos les consultarán al aplicar el Reglamento.

Debe ser posible modificar las orientaciones a la luz de la evolución y la práctica. A tal efecto, es fundamental que las autoridades de protección de datos promuevan una cultura de diálogo con todas las partes interesadas, incluidas las empresas.

²⁶ Todas las orientaciones adoptadas pueden consultarse en la siguiente dirección:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Es importante recordar que, cuando surjan cuestiones relativas a la interpretación y la aplicación del Reglamento, corresponderá a los órganos jurisdiccionales a escala nacional y de la UE ofrecer la interpretación final del Reglamento.

3. MEDIDAS PENDIENTES PARA UNA PREPARACIÓN SATISFACTORIA

3.1. Los Estados miembros deben ultimar el establecimiento del marco jurídico a nivel nacional

El Reglamento es directamente aplicable en todos los Estados miembros²⁷. Esto significa que entra en vigor y se aplica con independencia de cualquier medida legislativa nacional: por lo general, el Reglamento puede ser invocado directamente por los ciudadanos, empresas, administraciones públicas y otras organizaciones que tratan datos personales. No obstante, de conformidad con el Reglamento, los Estados miembros han de adoptar las medidas necesarias para adaptar su legislación mediante la derogación y modificación de las leyes existentes, así como implantando autoridades nacionales de protección de datos²⁸, eligiendo un organismo de acreditación²⁹ y estableciendo las normas para la conciliación de la libertad de expresión y la protección de los datos³⁰.

Asimismo, el Reglamento ofrece a los Estados miembros la posibilidad de precisar aún más la aplicación de las normas de protección de datos en sectores específicos: sector público³¹, empleo y seguridad social³², medicina preventiva y medicina laboral, sanidad pública³³, archivo con fines de interés público, investigación científica o histórica o con fines estadísticos³⁴, número nacional de identificación³⁵, acceso público a los documentos oficiales³⁶ y obligaciones de secreto³⁷. Además, en el caso de los datos genéticos, datos biométricos y datos relativos a la salud, el Reglamento autoriza a los Estados miembros a mantener o introducir condiciones adicionales, inclusive limitaciones³⁸.

Las acciones de los Estados miembros en este contexto quedan enmarcadas por dos elementos:

²⁷ Artículo 288 del TFUE.

²⁸ Artículo 54, apartado 1, del Reglamento.

²⁹ El artículo 43, apartado 1, del Reglamento establece que los Estados miembros ofrezcan dos posibles métodos de acreditación para los organismos de certificación, es decir, por la autoridad nacional de control de la protección de datos establecida de conformidad con la legislación de protección de datos, o bien por el organismo nacional de acreditación establecido en virtud del Reglamento (CE) n.º 765/2008 sobre acreditación y vigilancia del mercado. La Cooperación Europea para la Acreditación (EA, reconocida en virtud del Reglamento n.º 765/2008), que reúne a los organismos nacionales de acreditación, y las autoridades de control del RGPD deben cooperar estrechamente a tal efecto.

³⁰ Artículo 85, apartado 1, del Reglamento.

³¹ Artículo 6, apartado 2, del Reglamento.

³² Artículo 88 y artículo 9, apartado 2, letra b), del Reglamento. El pilar europeo de derechos sociales también afirma lo siguiente: «Los trabajadores tienen derecho a la protección de sus datos personales en el contexto del empleo». (2017/C 428/09, DO C 428 de 13.12.2017, pp. 10-15).

³³ Artículo 9, apartado 2, letras h) e i), del Reglamento.

³⁴ Artículo 9, apartado 2, letra j), del Reglamento.

³⁵ Artículo 87 del Reglamento.

³⁶ Artículo 86 del Reglamento.

³⁷ Artículo 90 del Reglamento.

³⁸ Artículo 9, apartado 4, del Reglamento.

1. el artículo 8 de la Carta, lo que significa que cualquier ley de especificación nacional debe cumplir los requisitos del artículo 8 de la Carta (y del Reglamento que se basa en el artículo 8 de la Carta), y
2. el artículo 16, apartado 2, del TFUE, en virtud del cual la legislación nacional no puede vulnerar la libre circulación de datos personales dentro de la UE.

El Reglamento supone la oportunidad para simplificar el entorno jurídico y, en consecuencia, tener un menor número de normas nacionales y una mayor claridad para los operadores.

Al adaptar su legislación nacional, los Estados miembros deben tener en cuenta que cualquier medida nacional que pueda obstaculizar la aplicabilidad directa del Reglamento y poner en peligro su aplicación simultánea y uniforme en el conjunto de la UE es contraria a los Tratados³⁹.

Asimismo, está prohibida la repetición del texto de los reglamentos en el Derecho nacional (por ejemplo, la repetición de las definiciones o los derechos de los individuos), salvo que sea estrictamente necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios⁴⁰. La reproducción literal del texto del Reglamento en la ley de especificación nacional debe ser excepcional y estar justificada, y no puede emplearse para añadir condiciones adicionales o interpretaciones al texto del Reglamento.

La interpretación del Reglamento compete a los órganos jurisdiccionales europeos (los tribunales nacionales y, en última instancia, el Tribunal de Justicia Europeo) y no a los legisladores de los Estados miembros. Por lo tanto, los legisladores nacionales no pueden ni copiar el texto del Reglamento cuando no sea necesario a la luz de los criterios establecidos por la jurisprudencia, ni interpretarlo o añadir condiciones adicionales a las normas directamente aplicables en virtud del Reglamento. Si lo hicieran, los operadores de toda la Unión se enfrentarían de nuevo a una situación de fragmentación y no sabrían qué normas deben cumplir.

En la fase actual, solo dos Estados miembros han adoptado ya la legislación nacional pertinente⁴¹; los demás Estados miembros se encuentran en distintas etapas de sus procedimientos legislativos⁴² y tienen programado adoptar la legislación antes del 25 de mayo de 2018. Es importante dar a los operadores tiempo suficiente para prepararse para todas las disposiciones que deben cumplir.

En caso de que los Estados miembros no adopten las medidas necesarias requeridas en virtud del Reglamento, se retrasen en su adopción o hagan uso de las cláusulas de especificación previstas en el Reglamento de manera contraria a lo dispuesto en él, la Comisión hará uso de todos los instrumentos que tiene a su disposición, incluido el recurso al procedimiento de infracción.

³⁹ Asunto 94/77, Fratelli Zerbone Snc/Amministrazione delle finanze dello Stato, ECLI:EU:C:1978:17 y 101.

⁴⁰ Considerando 8 del Reglamento.

⁴¹ Austria (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf) y Alemania (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#_bgbl_%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D_1513091793362).

⁴² Para una visión de conjunto de la situación en que se encuentra el proceso legislativo en los distintos Estados miembros, véase <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=ES>.

3.2. Las autoridades de protección de datos deben garantizar que el nuevo Comité Europeo de Protección de Datos independiente sea plenamente operativo

Es esencial que el nuevo organismo establecido por el Reglamento, el Comité Europeo de Protección de Datos⁴³, sucesor del Grupo de trabajo del artículo 29, sea plenamente operativo para el 25 de mayo de 2018.

El Supervisor Europeo de Protección de Datos, que es la autoridad de protección de datos responsable de la supervisión de las instituciones y organismos de la UE, asumirá la secretaría del Comité Europeo de Protección de Datos, con el fin de mejorar las sinergias y la eficacia. En los últimos meses, el Supervisor Europeo de Protección de Datos ha comenzado los preparativos necesarios a tal efecto.

El Comité Europeo de Protección de Datos será el punto de referencia de la protección de datos en Europa. Contribuirá a una aplicación coherente de la legislación en materia de protección de datos y proporcionará una base sólida para la cooperación entre las autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos. El Comité Europeo de Protección de Datos no solo publicará orientaciones sobre cómo interpretar los conceptos básicos del Reglamento, sino que también se le pedirá que emita decisiones vinculantes sobre conflictos relativos al tratamiento transfronterizo. Esto garantizará la aplicación uniforme de las normas de la UE y evitará que el mismo caso se trate de forma diferente en los distintos Estados miembros.

Así pues, el funcionamiento eficiente y fluido del Comité Europeo de Protección de Datos es requisito para que el sistema en su conjunto funcione correctamente. Ahora más que nunca, el Comité Europeo de Protección de Datos deberá crear una cultura común de protección de datos entre todas las autoridades nacionales de protección de datos para garantizar que las disposiciones del Reglamento se interpretan de manera coherente. El Reglamento fomenta la cooperación entre las autoridades de protección de datos, dándoles las herramientas para cooperar de manera eficaz y eficiente: concretamente, podrán realizar operaciones conjuntas, adoptar decisiones de común acuerdo y subsanar las divergencias que pudieran tener en relación con la interpretación del Reglamento en el seno del Comité por medio de dictámenes y decisiones vinculantes. La Comisión anima a las autoridades de protección de datos a adoptar estos cambios y a adaptar su funcionamiento, su financiación y su cultura de trabajo para poder cumplir con los nuevos derechos y obligaciones.

3.3. Los Estados miembros deben facilitar los recursos financieros y humanos necesarios a las autoridades nacionales de protección de datos

La creación de autoridades de control totalmente independientes en cada Estado miembro es fundamental para garantizar la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales en la UE⁴⁴. Las autoridades de control no pueden salvaguardar de manera efectiva los derechos y libertades individuales a menos que actúen con total independencia. Cualquier fallo a la hora de garantizar su independencia y el ejercicio

⁴³ El Comité Europeo de Protección de Datos será un organismo de la UE con personalidad jurídica encargado de velar por la aplicación coherente del Reglamento. Estará compuesto por el director de cada autoridad de protección de datos y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes.

⁴⁴ Considerando 117, y establecido anteriormente en el considerando 62 de la Directiva 95/46.

efectivo de sus competencias tiene una gran repercusión negativa sobre la aplicación de la legislación en materia de protección de datos⁴⁵.

El Reglamento codifica el requisito de que toda autoridad de protección de datos actúe de forma completamente independiente⁴⁶. Refuerza la independencia de las autoridades nacionales de protección de datos y les otorga competencias uniformes en toda la UE, a fin de que estén adecuadamente equipadas para tratar de manera efectiva las reclamaciones, llevar a cabo investigaciones eficaces, tomar decisiones vinculantes e imponer sanciones efectivas y disuasorias. También les confiere la facultad de aplicar multas administrativas a los responsables del tratamiento o a los encargados de hasta 20 millones EUR o, en el caso de una empresa, de hasta el 4 % del volumen de negocios total a nivel mundial del ejercicio fiscal anterior, la cifra que resulte más elevada.

Las autoridades de protección de datos son los interlocutores naturales y el primer punto de contacto para los ciudadanos, las empresas y las administraciones públicas en cuanto a consultas relacionadas con el Reglamento. El papel de las autoridades de protección de datos incluye informar a los responsables y a los encargados del tratamiento sobre sus obligaciones y aumentar la sensibilización del público en general y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de los datos. No obstante, esto no significa que los responsables y los encargados del tratamiento deban esperar que las autoridades de protección de datos les proporcionen el tipo de asesoramiento jurídico personalizado e individualizado que solo un abogado o un responsable de la protección de datos puede ofrecer.

Por lo tanto, las autoridades nacionales de protección de datos desempeñan un papel fundamental, pero el desequilibrio relativo entre los recursos humanos y financieros que se les asignen en los distintos Estados miembros puede poner en peligro su eficacia, y, en última instancia, la independencia total exigida por el Reglamento. También puede repercutir negativamente en el modo en que las autoridades de protección de datos pueden ejercer competencias tales como sus funciones de investigación. Se anima a los Estados miembros a cumplir con su obligación legal de proporcionar a su autoridad nacional de protección de datos los recursos humanos, técnicos y financieros, así como las instalaciones e infraestructuras, necesarios para el desempeño efectivo de sus funciones y el ejercicio de sus competencias⁴⁷.

3.4. Las empresas, las administraciones públicas y otras organizaciones que tratan datos deben prepararse para la aplicación de las nuevas normas

El Reglamento no ha modificado de manera sustancial los conceptos y principios básicos de la legislación en materia de protección de datos establecida en 1995. Esto debería significar que la gran mayoría de los responsables y encargados del tratamiento, siempre que cumplan ya la legislación vigente de la UE en materia de protección de datos, no necesitarán realizar cambios importantes en sus operaciones de tratamiento de datos para cumplir el Reglamento.

⁴⁵ Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, COM(2007) 87 final, de 7 de marzo de 2007.

⁴⁶ Artículo 52 del Reglamento.

⁴⁷ Artículo 52, apartado 4, del Reglamento.

El Reglamento afecta más a los operadores cuya actividad principal es el tratamiento o manejo de datos sensibles. También repercute en aquellos que regular y sistemáticamente realizan un seguimiento de individuos a gran escala. Estos operadores deberán, con toda probabilidad, nombrar a un delegado de protección de datos, llevar a cabo una evaluación de impacto relativa a la protección de datos y notificar cualquier violación de la seguridad de los datos si existe un riesgo para los derechos y libertades de las personas. En cambio, los operadores, en concreto las pymes, que no realizan tratamientos de datos de alto riesgo como actividad principal, por lo general no estarán sujetos a estas obligaciones específicas del Reglamento.

Es importante que los responsables y los encargados del tratamiento revisen en profundidad el ciclo de su política de datos a fin de determinar claramente los datos de los que disponen, con qué objeto y sobre qué base jurídica (p. ej. la computación en nube u operadores del sector financiero). También tienen que evaluar los contratos vigentes, en concreto aquellos entre responsables y encargados del tratamiento, las vías para las transferencias internacionales y la gobernanza general (qué medidas organizativas y medidas en el campo de la informática van a aplicarse), incluido el nombramiento de un delegado de protección de datos. Un elemento fundamental de este proceso es garantizar que la dirección de más alto nivel participa en dichas revisiones, aporta su contribución y se la mantiene informada y se la consulta periódicamente sobre los cambios en la política de datos de la empresa.

A tal fin, algunos operadores recurren a listas de comprobación del cumplimiento (tanto interno como externo), solicitan asesoramiento a sociedades de consultoría y bufetes de abogados y buscan productos que se adecuen a los requisitos de protección de datos desde el diseño y por defecto. Cada sector debe elaborar mecanismos que sean adecuados a la naturaleza específica de su ámbito y que se adapten a su modelo de negocio.

Las empresas y otras organizaciones que realizan el tratamiento de datos también podrán aprovechar las nuevas herramientas previstas en el Reglamento como elemento para demostrar el cumplimiento, tales como códigos de conducta y mecanismos de certificación. Estas constituyen planteamientos ascendentes que proceden de la comunidad empresarial, asociaciones u otras organizaciones que representan a categorías de responsables o encargados del tratamiento y reflejan las mejores prácticas, avances importantes en un sector determinado, o pueden informar sobre el nivel de protección de datos exigido por determinados productos y servicios. El Reglamento prevé un conjunto simplificado de normas para tales mecanismos, al tiempo que tiene en cuenta la realidad del mercado (p.ej. la certificación por un organismo de certificación o por una autoridad de protección de datos).

Sin embargo, mientras que las grandes empresas están preparándose activamente para la aplicación de las nuevas normas, muchas pymes todavía no conocen del todo las futuras normas en materia de protección de datos.

En resumen, los operadores deben prepararse y adaptarse a las nuevas normas y ver el Reglamento como:

- una oportunidad para poner orden en sus actividades en lo referente a los datos personales que tratan y cómo lo gestionan;
- una obligación para desarrollar productos compatibles con la privacidad y la protección de los datos y para construir una nueva relación con sus consumidores basada en la transparencia y la confianza; así como
- una oportunidad para restablecer sus relaciones con las autoridades de protección de datos a través de la rendición de cuentas y el cumplimiento proactivo.

3.5. Informar a las partes interesadas, en particular a los ciudadanos y a las pymes

El éxito del Reglamento depende de la adecuada sensibilización de todos aquellos a quienes conciernen las nuevas normas (la comunidad empresarial y otras organizaciones que realizan el tratamiento de datos, el sector público y los ciudadanos). A nivel nacional, la tarea de sensibilizar y de actuar como primer punto de contacto para los responsables del tratamiento, los encargados y los particulares recae principalmente en las autoridades de protección de datos. Como garantes del cumplimiento de las normas de protección de datos en su territorio, las autoridades de protección de datos son también las mejor situadas para explicar los cambios introducidos por el Reglamento a las empresas y al sector público, así como para dar a conocer a los ciudadanos sus derechos.

Las autoridades de protección de datos han empezado a informar a las partes interesadas de acuerdo con el planteamiento nacional específico. Algunas organizan seminarios con las administraciones públicas, también a nivel regional y local, y organizan talleres con distintos sectores empresariales a fin de aumentar la sensibilización sobre las principales disposiciones del Reglamento. Otras realizan programas de formación específicos para delegados de protección de datos. La mayoría de ellas ofrecen material informativo en distintos formatos en sus sitios web (listas de comprobación, vídeos, etc.).

Sin embargo, todavía no existe entre los ciudadanos un nivel de sensibilización suficientemente generalizado sobre los cambios y las mejoras en los derechos que las nuevas normas de protección de datos traerán consigo. La iniciativa de formación y sensibilización puesta en marcha por las autoridades de protección de datos debería mantenerse e intensificarse, con un especial hincapié en las pymes. Por otra parte, las administraciones sectoriales nacionales pueden respaldar las actividades de las autoridades de protección de datos y, sobre la base de la información que estas aporten, llevar a cabo sus propias actividades de divulgación dirigidas a las distintas partes interesadas.

4. PRÓXIMAS ETAPAS

En los próximos meses, la Comisión seguirá apoyando activamente a todos los actores en la preparación de la aplicación del Reglamento.

a) Trabajo con los Estados miembros

La Comisión seguirá trabajando con los Estados miembros en el periodo previo a mayo de 2018. De mayo de 2018 en adelante, realizará un seguimiento de la aplicación de las nuevas normas por los Estados miembros y adoptará las medidas apropiadas cuando sea necesario.

b) Nuevas orientaciones en línea en todas las lenguas de la UE y actividades de sensibilización

La Comisión está elaborando materiales prácticos de orientación⁴⁸ para ayudar a las empresas, en particular a las pymes, las autoridades públicas y los ciudadanos a cumplir las nuevas normas de protección de datos y a beneficiarse de ellas.

Las orientaciones adoptan la forma de una herramienta práctica en línea disponible en todas las lenguas de la UE. Esta herramienta en línea se actualizará periódicamente y está destinada a ayudar a tres públicos destinatarios principales: los ciudadanos, las empresas (en concreto las pymes) y otras organizaciones y las administraciones públicas. Se compone de preguntas y respuestas seleccionadas en función de los comentarios recibidos de las partes interesadas, con ejemplos prácticos y enlaces a distintas fuentes de información (p. ej. artículos del Reglamento; orientaciones del Grupo de trabajo del artículo 29 o Comité Europeo de Protección de Datos; y materiales elaborados a nivel nacional).

La Comisión actualizará periódicamente la herramienta, añadiendo preguntas y poniendo al día las respuestas, con arreglo a los comentarios recibidos y a las nuevas cuestiones que puedan surgir de su aplicación.

Las orientaciones se promoverán a través de una campaña de información y de actividades de divulgación en todos los Estados miembros, destinadas a las empresas y a los ciudadanos.

Ya que el Reglamento establece derechos individuales más fuertes, la Comisión llevará a cabo también actividades de sensibilización y participará en actos en los distintos Estados miembros para informar a los ciudadanos sobre las consecuencias y las ventajas del Reglamento.

c) Apoyo financiero a las campañas y las actividades de sensibilización nacionales

La Comisión apoya los esfuerzos de sensibilización y cumplimiento emprendidos a nivel nacional mediante la concesión de subvenciones que pueden emplearse para proporcionar formación en los ámbitos de las autoridades de protección de datos, las administraciones públicas, las profesiones jurídicas y los delegados de protección de datos⁴⁹ a fin de que se familiaricen con el Reglamento.

Se asignarán alrededor de 1,7 millones EUR a seis beneficiarios, que cubrirán más de la mitad de los Estados miembros de la UE. La financiación se destinará a las autoridades públicas locales, incluidos los delegados de protección de datos de dichas autoridades, de las autoridades públicas y del sector privado, así como a jueces y abogados. Las subvenciones se emplearán para elaborar materiales de formación para las autoridades de protección de datos, los delegados de protección de datos y otros profesionales, así como para programas de «formación de formadores».

⁴⁸ Las orientaciones contribuirán a una mejor comprensión de las normas de protección de datos de la UE, pero únicamente el texto del Reglamento tiene validez jurídica. En consecuencia, solo el Reglamento puede generar derechos y obligaciones para los individuos.

⁴⁹ Subvenciones concedidas en el marco del Programa de Derechos y Ciudadanía para 2016: <https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c.topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identfier/desc>.

La Comisión también ha publicado una convocatoria de propuestas dirigida específicamente a las autoridades de protección de datos. Dispondrá de un presupuesto total de hasta 2 millones EUR y las apoyará facilitándoles el contacto con las partes interesadas⁵⁰. El objetivo es proporcionar una cofinanciación del 80 % a las medidas adoptadas por las autoridades de protección de datos para el periodo 2018-2019 con el fin de sensibilizar a las empresas, en particular a las pymes, y de responder a sus consultas. Esta financiación puede utilizarse también para sensibilizar al público en general.

d) Evaluar la necesidad de servirse de las facultades de la Comisión

El Reglamento⁵¹ permite a la Comisión elaborar actos de ejecución o actos delegados con el fin de apoyar aún más la aplicación de las nuevas normas. La Comisión solo hará uso de estas facultades cuando exista un valor añadido claramente demostrado y basado en la información obtenida de la consulta a las partes interesadas. En concreto, la Comisión examinará la cuestión de la certificación basándose en un estudio contratado con expertos externos y en las aportaciones y el asesoramiento sobre el tema recibidos del grupo multilateral sobre el Reglamento establecido a finales de 2017. En este contexto, también será relevante el trabajo realizado por la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) en el ámbito de la ciberseguridad.

e) Integración del Reglamento en el Acuerdo sobre el Espacio Económico Europeo

La Comisión proseguirá su trabajo con los tres Estados de la AELC (Islandia, Liechtenstein y Noruega) en el Espacio Económico Europeo (EEE) para integrar el Reglamento en el Acuerdo EEE⁵². Solo cuando la integración del Reglamento en el Acuerdo EEE entre en vigor podrán los datos personales circular libremente entre países de la UE y del EEE de la misma manera en que lo hacen entre los Estados miembros de la UE.

f) Retirada del Reino Unido de la UE

En el contexto de las negociaciones de un acuerdo de retirada entre la UE y el Reino Unido en virtud del artículo 50 del Tratado de la Unión Europea, la Comisión perseguirá el objetivo de garantizar que las disposiciones del Derecho de la Unión sobre la protección de los datos personales aplicables el día anterior a la fecha de la retirada sigan aplicándose a los datos personales tratados en el Reino Unido antes de la fecha de la retirada⁵³. Por ejemplo, las personas afectadas deben seguir teniendo el derecho a ser informadas, derecho de acceso, de rectificación, de eliminación, de limitación del tratamiento, derecho a la portabilidad de los

⁵⁰ <http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html>

⁵¹ Acto delegado relativo a la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados (artículo 12, apartado 8, del Reglamento); acto delegado relativo a las condiciones que deberán tenerse en cuenta para los mecanismos de certificación (artículo 43, apartado 8, del Reglamento); acto de ejecución para establecer normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas (artículo 43, apartado 9, del Reglamento); acto de ejecución para especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes (artículo 47, apartado 3, del Reglamento); actos de ejecución para especificar el formato y los procedimientos de asistencia mutua y para el intercambio de información por medios electrónicos entre las autoridades de control (artículo 61, apartado 9, y artículo 67 del Reglamento).

⁵² Para más información sobre la situación actual, véase www.efta.int/eea-lex/32016R0679.

⁵³ https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_es

datos, así como derecho a oponerse al tratamiento y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de los datos, de acuerdo con las disposiciones pertinentes del Derecho de la Unión aplicables en la fecha de la retirada. Los datos personales mencionados anteriormente deben almacenarse durante un período no superior al estrictamente necesario para los fines para los que se trataron.

A partir de la fecha de retirada, y sin perjuicio de cualquier disposición transitoria que pueda estar contenida en un posible acuerdo de retirada, las normas del Reglamento para las transferencias de datos personales a terceros países se aplicarán al Reino Unido⁵⁴.

g) Balance en mayo de 2019

A partir del 25 de mayo de 2018, la Comisión supervisará de cerca la aplicación de las nuevas normas y estará preparada para tomar medidas en caso de que surjan problemas importantes. Un año después del comienzo de la aplicación del Reglamento (en 2019), la Comisión organizará un acto para hacer balance de las experiencias de las distintas partes interesadas por lo que respecta a la aplicación del Reglamento. Este balance se incorporará también al informe que la Comisión debe preparar para mayo de 2020 sobre la evaluación y revisión del Reglamento. Dicho informe se centrará, en concreto, en las transferencias internacionales y en las disposiciones sobre cooperación y coherencia que atañen al trabajo de las autoridades de protección de datos.

Conclusión

El 25 de mayo, un nuevo conjunto único de normas de protección de datos empezará a aplicarse de manera efectiva en toda la UE. El nuevo marco reportará importantes beneficios para los particulares, las empresas, las administraciones públicas y otras organizaciones similares. Constituye también una oportunidad para que la UE se convierta en líder mundial en materia de protección de datos personales. Pero la reforma solo puede tener éxito si todas las partes implicadas asumen sus obligaciones y sus derechos.

Desde la adopción del Reglamento en mayo de 2016, la Comisión ha colaborado activamente con todos los actores interesados (gobiernos, autoridades nacionales, empresas y sociedad civil) con vistas a la aplicación de las nuevas normas. Se ha dedicado una importante cantidad de trabajo a garantizar la sensibilización generalizada y una preparación completa, pero todavía queda trabajo por hacer. Los preparativos avanzan con distinto ritmo en los diferentes Estados miembros y según los diversos actores. Por otra parte, los beneficios y las oportunidades que brinda la nueva normativa no se conocen en todas partes por igual. Se observa, en concreto, que es preciso incrementar la sensibilización de las pymes y acompañar sus esfuerzos de cumplimiento.

Así pues, la Comisión insta a todos los actores interesados a intensificar el trabajo que ya se está realizando para garantizar la aplicación y la interpretación coherentes de las nuevas normas en toda la UE, así como para sensibilizar a los ciudadanos y las empresas. La Comisión respaldará estos esfuerzos con financiación y apoyo administrativo y contribuirá a la labor de divulgación general, en particular mediante la puesta en funcionamiento de las herramientas de orientación en línea.

⁵⁴ Véase la Comunicación de la Comisión a las partes interesadas: retirada del Reino Unido y las normas de la UE en el ámbito de la protección de datos (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

Los datos se están convirtiendo en algo muy valioso para la economía actual y son fundamentales para la vida cotidiana de los ciudadanos. Las nuevas normas ofrecen una oportunidad única tanto para las empresas como para los ciudadanos. Las empresas, especialmente las más pequeñas, podrán beneficiarse del conjunto único de normas favorables a la innovación y podrán organizar sus actividades internas en lo que respecta a datos personales, para restablecer la confianza del consumidor y emplearla para su ventaja competitiva en toda la UE. Los ciudadanos podrán beneficiarse de una mayor protección de los datos personales y adquirir un mayor control sobre el manejo de los datos por las empresas.

En un mundo moderno con una economía digital en auge, la Unión Europea, sus ciudadanos y las empresas deben estar plenamente equipados para aprovechar las ventajas y comprender las consecuencias de la economía de los datos. El nuevo Reglamento ofrece las herramientas necesarias para crear una Europa equipada para el siglo XXI.

La Comisión llevará a cabo las siguientes acciones:

En relación con los Estados miembros

- La Comisión seguirá trabajando con los Estados miembros para fomentar la coherencia y limitar la fragmentación en la aplicación del Reglamento, teniendo en cuenta el margen de especificación de que disponen los Estados miembros en virtud de la nueva legislación;
- después de mayo de 2018, la Comisión supervisará de cerca la aplicación del Reglamento en los Estados miembros y adoptará las medidas adecuadas cuando sea necesario, incluido el recurso a las acciones por infracción.

En relación con las autoridades de protección de datos

- Hasta mayo de 2018, la Comisión apoyará la labor de las autoridades de protección de datos en el contexto del Grupo de trabajo del artículo 29 y en la transición hacia el futuro Comité Europeo de Protección de Datos; después de mayo de 2018, contribuirá al trabajo del Comité Europeo de Protección de Datos;
- en el periodo 2018-2019, la Comisión cofinanciará (con un presupuesto total de hasta 2 millones EUR) las acciones de sensibilización llevadas a cabo por las autoridades de protección de datos a nivel nacional (proyectos ejecutados a partir de mediados de 2018).

En relación con las partes interesadas

- La Comisión pondrá en funcionamiento una herramienta de orientación práctica en línea que incluye preguntas y respuestas dirigidas a los ciudadanos, las empresas y las administraciones públicas. La Comisión piensa promover estas orientaciones de cara al público destinatario a través de una campaña de información dirigida a las empresas y al público en el periodo previo a mayo de 2018 y posteriormente;
- en 2018 y a partir de entonces, la Comisión seguirá trabajando activamente con las partes interesadas, en concreto a través del grupo multilateral sobre la aplicación del Reglamento y el nivel de sensibilización hacia las nuevas normas.

En relación con todos los actores

- En 2018 y 2019, la Comisión evaluará la necesidad de hacer uso de sus competencias para adoptar actos delegados o de ejecución;
- en mayo de 2019, la Comisión hará un balance de la aplicación del Reglamento y elaborará un informe sobre la aplicación de las nuevas normas en 2020.