Consejo de la UE

PRESS
ES

COMUNICADO DE PRENSA
951/15
18.12.2015

Reforma de la protección de datos en la UE: el Consejo confirma el acuerdo con el Parlamento Europeo

El 18 de diciembre de 2015, el Comité de Representantes Permanentes (Coreper) ha confirmado los textos transaccionales acordados con el Parlamento Europeo sobre la reforma de la protección de datos. El Consejo, el Parlamento y la Comisión alcanzaron el acuerdo el 15 de diciembre. El acuerdo se ajusta a la petición del Consejo Europeo de que se concluyeran las negociaciones acerca de la reforma de la protección de datos a finales de 2015 a más tardar.

Félix Braz, ministro de Justicia de Luxemburgo y presidente del Consejo, ha comentado: «Es un acuerdo fundamental con consecuencias importantes. Esta reforma no solo refuerza los derechos de los ciudadanos, sino también adapta a la era digital la normativa para las empresas, al tiempo que reduce la carga administrativa. Se trata de textos ambiciosos y con visión de futuro. Podemos tener plena confianza en el resultado».

La reforma de la protección de datos es un conjunto legislativo que en 2012 propuso la Comisión para actualizar y modernizar la normativa sobre protección de datos. Afecta a dos instrumentos legislativos: el Reglamento general de protección de datos (destinado a sustituir la Directiva 95/46/CE) y la Directiva sobre protección de datos en el ámbito policial (destinada a sustituir la Decisión marco sobre protección de datos de 2008).

La protección de las personas en relación con el tratamiento de sus datos personales es un derecho fundamental consagrado en la Carta de los Derechos Fundamentales de la UE (artículo 8) y en el Tratado de Funcionamiento de la Unión Europea (artículo 16).

Reglamento general de protección de datos

El Reglamento general de protección de datos tiene por objeto mejorar el nivel de protección de los datos de las personas físicas cuyos datos personales se someten a tratamiento y aumentar las oportunidades de negocio en el mercado único digital, en particular mediante la reducción de la carga administrativa.

Mejora del nivel de protección de los datos

Los principios y normas sobre el tratamiento de los datos personales de las personas físicas deben respetar los derechos y libertades fundamentales, en particular el derecho a la protección de los datos de carácter personal. Este refuerzo de los derechos en materia de protección de datos ofrece a los interesados (las personas físicas cuyos datos personales se someten a tratamiento) un mayor control sobre sus datos de carácter personal:

- Normas más específicas que permitan que los responsables del tratamiento (los encargados de someter a tratamiento los datos) traten datos de carácter personal, en particular mediante la exigencia del consentimiento de las personas físicas afectadas.
- Un acceso más fácil a sus datos personales.
- La mejora de la información acerca de lo que ocurre con los datos personales cuando se comparten, en particular informando a las personas físicas acerca de las políticas de privacidad en un lenguaje claro y sencillo o mediante iconos normalizados.
- El derecho a la supresión de los datos personales y «al olvido», que permite, por ejemplo, que los interesados exijan la supresión, sin demora, de datos personales recogidos o publicados en una red social cuando la persona en cuestión todavía era un niño.
- Si un menor de dieciséis años quiere utilizar servicios en línea, el proveedor del servicio deberá intentar comprobar que los padres hayan dado su consentimiento. Los Estados miembros podrán reducir ese límite de edad sin bajar de los trece años.
- El derecho a la portabilidad, que facilita la transmisión de datos personales de un proveedor de servicios, como una red social, a otro. Esto no solo aumentará los derechos en materia de protección de datos, sino que también mejorará la competencia entre proveedores de servicios.
- El derecho a oponerse al tratamiento de datos personales relacionado con el interés público o con los intereses legítimos del responsable del tratamiento. Este derecho abarca el uso de datos de carácter personal a efectos de la «elaboración de perfiles».
- Salvaguardias comunes que afectan al tratamiento de datos personales con fines de archivo por razones de interés público o para fines de investigación científica e histórica o estadísticos.

Para garantizar la proximidad del recurso jurídico, los interesados tendrán derecho a que las decisiones de su autoridad de protección de datos sean revisadas por sus tribunales nacionales, con independencia del Estado miembro en que esté establecido el responsable del tratamiento.

Aumento de las posibilidades de negocio en el mercado único digital

El Reglamento establece una normativa única, válida en toda la UE y aplicable tanto a las empresas europeas como a las no europeas que ofrezcan servicios en línea en la UE. Se evita así una situación en la que unas normas nacionales contradictorias en materia de protección de datos pudieran alterar el intercambio transfronterizo de datos. Asimismo, prevé el refuerzo de la cooperación entre los Estados miembros a fin de garantizar la aplicación coherente de las normas de protección de datos en toda la UE. Esto generará una competencia leal y animará a las empresas, sobre todo a las pequeñas y medianas, a sacar el máximo provecho del mercado único digital.

Para reducir costes y crear seguridad jurídica, en los casos transfronterizos importantes en los que intervengan varias autoridades nacionales de control, se adoptará una decisión de control única. Este **mecanismo de ventanilla única** permite que una empresa activa en varios Estados miembros trate únicamente con la autoridad de protección de datos del Estado miembro de su establecimiento principal. Ese mecanismo prevé asimismo una decisión única aplicable a todo el territorio de la UE en caso de disputas.

Con objeto de reducir los costes administrativos, el Reglamento aplica un enfoque basado en los riesgos: los responsables del tratamiento pueden poner en práctica medidas de acuerdo con el riesgo que impliquen las operaciones de tratamiento de datos que lleven a cabo. Las distintas empresas tienen distintas actividades, y los riesgos de esas actividades en lo que se refiere a la intimidad pueden variar. El Reglamento no ofrece una solución única válida para todos los casos: cuanto mayores riesgos supongan las actividades para los datos personales, más estrictas serán las obligaciones.

Aumento y mejora de los instrumentos para garantizar el cumplimiento de las normas de protección de datos

El Reglamento establece una serie de medidas para aumentar la responsabilidad y la rendición de cuentas de los responsables del tratamiento a fin de garantizar el pleno cumplimiento de las nuevas normas de protección de datos. Los responsables del tratamiento deben poner en práctica una serie de medidas de seguridad, incluida la obligación de notificar las violaciones de datos personales en determinados casos. Para que el Reglamento resista el paso del tiempo, se introducen los principios de protección de datos desde el diseño y por defecto. Las autoridades públicas y aquellas empresas que lleven a cabo determinados tratamientos de datos que supongan un riesgo deberán designar a un **responsable de la protección de datos** para garantizar el cumplimiento de la normativa.

Los interesados y, en determinadas condiciones, las organizaciones de protección de datos podrán presentar reclamaciones ante una autoridad de control o interponer un recurso en caso de que no se cumplan las normas de protección de datos. Los responsables del tratamiento pueden enfrentarse a multas de hasta 20 millones de euros o el 4 % de su volumen de negocios anual mundial.

Garantías para la transferencia de datos personales al exterior de la UE

El Reglamento establece las normas para la transferencia de datos personales a terceros países y organizaciones internacionales. Las transferencias pueden llevarse a cabo siempre que se cumpla una serie de condiciones y salvaguardias, en particular cuando la Comisión haya decidido que existe un nivel adecuado de protección. Las nuevas decisiones sobre el carácter adecuado de la protección tendrán que revisarse al menos cada cuatro años. Las autorizaciones y decisiones sobre el carácter adecuado de la protección existentes seguirán en vigor hasta que se modifiquen, sustituyan o deroguen.

Directiva sobre protección de datos en el ámbito policial

Esta Directiva tiene por objeto proteger los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y prevención frente a amenazas contra la seguridad pública.

Es fundamental garantizar un nivel uniforme y elevado de protección de los datos personales de las personas físicas al tiempo que se facilita el intercambio de datos personales entre las autoridades policiales de los distintos Estados miembros.

Ampliación del ámbito de aplicación

Además de abarcar actividades destinadas a prevenir, investigar, detectar y enjuiciar infracciones penales, se ha ampliado el ámbito de aplicación de la nueva Directiva para que también cubra la protección y prevención de amenazas para la seguridad pública.

La nueva Directiva se aplicará tanto al tratamiento transfronterizo de datos personales como al tratamiento de datos personales

por las autoridades policiales y judiciales en el ámbito meramente nacional. La Decisión marco, que quedará sustituida, cubría únicamente el intercambio transfronterizo de datos.

Derechos de los interesados

Las normas logran un equilibrio entre el derecho a la intimidad y la necesidad de que la policía no revele que se están tratando datos al comienzo de una investigación. No obstante, el texto enumera la información que el interesado siempre tiene derecho a recibir a fin de proteger sus derechos si teme que se ha producido una infracción en lo que respecta a sus datos.

Las nuevas normas también abarcarán la transferencia de datos personales a terceros países y organizaciones internacionales.

Cumplimiento

La nueva Directiva prevé el nombramiento de un **responsable de la protección de datos** para ayudar a las autoridades competentes a garantizar el cumplimiento de la normativa sobre protección de datos.

Otro instrumento para garantizar el cumplimiento es la evaluación de impacto. Cuando sea probable que un tipo de tratamiento suponga un riesgo elevado para los derechos y las libertades de personas físicas, las autoridades competentes deberán llevar a cabo una evaluación del posible impacto de un tratamiento determinado, en particular cuando se utilice una tecnología nueva.

Supervisión e indemnización

El texto de la Directiva está en consonancia con el texto del Reglamento para garantizar que, a grandes rasgos, se apliquen los mismos principios generales. Además, las normas sobre la autoridad de control son en gran medida similares, ya que la autoridad de control establecida en el Reglamento general de protección de datos también puede ocuparse de los asuntos que competen a la Directiva. La nueva Directiva garantizaría también a los interesados el derecho a ser indemnizados si hubieran sufrido perjuicios como consecuencia de un tratamiento no conforme a las normas.

SIGUIENTES ETAPAS

El 17 de diciembre, en una reunión extraordinaria, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) aprobó los textos acordados en los diálogos tripartitos. Este apoyo ha permitido que el Coreper confirme hoy los textos transaccionales definitivos del Reglamento y la Directiva. Tras la revisión jurídico-lingüística de los textos, estos se presentarán para su adopción por el Consejo y, posteriormente, por el Parlamento. Probablemente el Reglamento y la Directiva entrarán en vigor en la primavera de 2018.

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press