Europar Erreglamendu bateratua?
Ez berdintasunak gaur egungo datuak babesteko araudiarekiko.

Reglamento Europeo, ¿Unificado? Diferencias respecto a la vigente normativa de protección de datos

DATA PROTECTION AND NEW EUROPEAN REGULATION
General Data Protection Regulation - GDPR

DATUEN BABESA ETA EUROPAKO ERREGLAMENDU BERRIA
Datuen Babeserako Erreglamendu Orokorra – DBEO

PROTECCIÓN DE DATOS Y SU NUEVO REGLAMENTO EUROPEO
Reglamento General de Protección de Datos - RGPD

Camino recorrido...

LORTAD

5/1992

994/1999

15/1999

1720/2007

RDLOPD

LOPD

Directiva 46/95/CE

RGPD

Órgano PARLAMENTO Y CONSEJO DE LA UNION EUROPEA

Publicado en DOUEL núm. 119 de 04 de Mayo de 2016

Vigencia desde 05 de Mayo de 2016

173 considerandos y 99 artículos

#GDPR #DPO

#EU/2016/679

2012-2016

25 mayo 2018

biantik

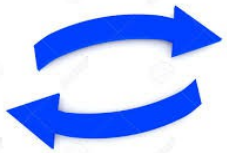
Europar Erreglamendu bateratua?
Reglamento Europeo, ¿Unificado?

Directiva 46/95/CE

VS

European Commission

GDPR - EU/2016/679



El efecto directo del Derecho europeo

Europar Erreglamendu bateratua?
Reglamento Europeo, ¿Unificado?

Considerando 73: El Derecho de la Unión o de los Estados miembros puede imponer restricciones:

- A determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales.
- Al derecho a la portabilidad de los datos.
- Al derecho de oposición.
- A las decisiones basadas en la elaboración de perfiles.
- A la comunicación de una violación de la seguridad de los datos personales a un interesado.
- A determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano.

Europar Erreglamendu bateratua?
Reglamento Europeo, ¿Unificado?

Considerando 73: El Derecho de la Unión o de los Estados miembros puede imponer restricciones:

- La prevención, investigación y el enjuiciamiento de infracciones penales.
- La ejecución de sanciones penales.
- La protección frente a las amenazas contra la seguridad pública.
- Las violaciones de normas deontológicas en las profesiones reguladas, y su prevención.
- Otros objetivos importantes de interés público general de la Unión o de un Estado miembro.
- En particular un importante interés económico o financiero de la Unión o de un Estado miembro.

  ¿Qué quiere decir? ¿Hablamos del TTIP? ¿Intereses de un Estado miembro?
- La llevanza de registros públicos por razones de interés público general.

biantik

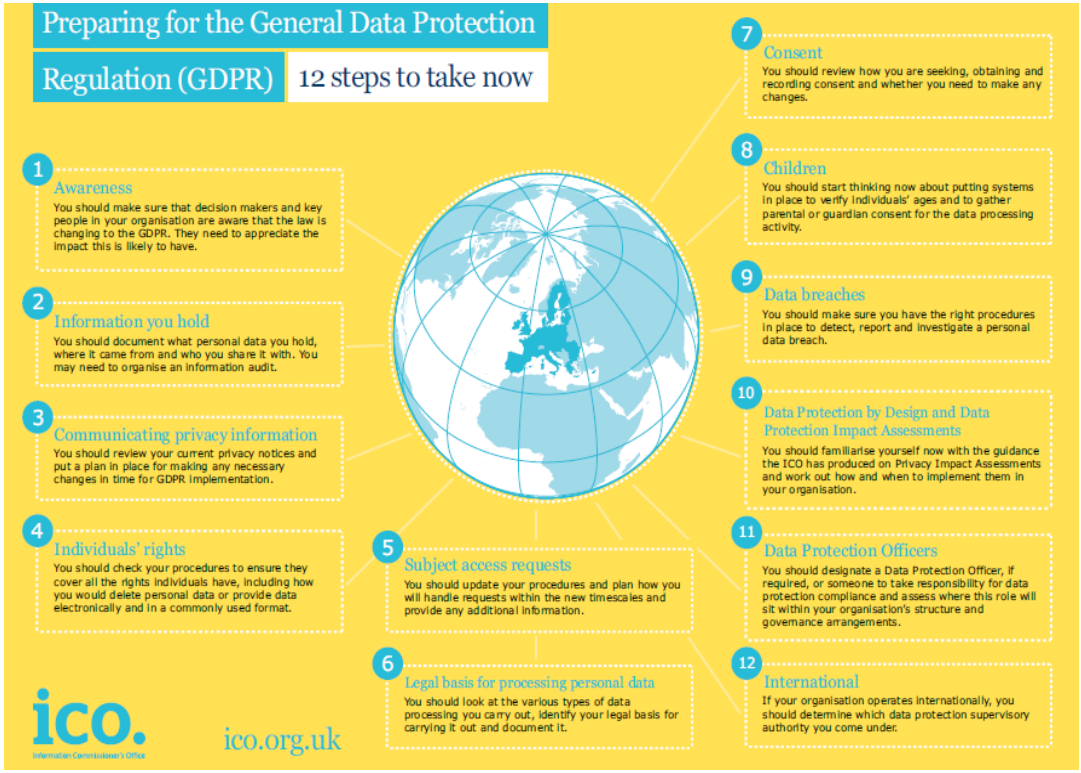
Europar Erreglamendu bateratua?
Reglamento Europeo, ¿Unificado?

Considerando 73: El Derecho de la Unión o de los Estados miembros puede imponer restricciones:

- El tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios.
- La protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios.

Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

biantik



1. Concienciación
2. La información almacenada
3. Comunicación de privacidad
4. Derechos individuales
5. Solicitud de accesos
6. Mínimos legales para tratar DP
7. Consentimiento
8. Menores
9. Brechas de seguridad
10. PD desde el diseño y PIA
11. DPO Data Protecction Officers
12. Internacional

ico.
Information Commissioner's Office

https://ico.org.uk/

ISO 27001

Polémica...

biantik

Sentencia TJUE 03/10/2015

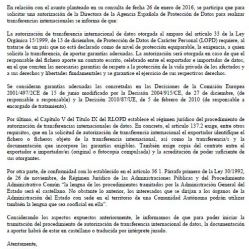
Maximillian Schrems,

Decisión de 26 de julio de 2000

Carta de los Derechos Fundamentalesde la Unión Europea

Directiva 46/95/CE

U.S. • EU
SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE



U.S. • EU
SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE
INVALID

Marcel Lettre

Oficina del Director de Inteligencia Nacional de EEUU (ODNI)

Privacy Shield

Article 29
Working Party

The **Article 29 Data Protection Working Party** was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the **protection of individuals** with regard to the **processing of personal data** and on the **free movement** of such data.

It has advisory status and acts independently.

Algunos preceptos, consentimiento

Artículo 7 Condiciones para el consentimiento

7.1...el **responsable deberá ser capaz de demostrar que aquel consintió** el tratamiento de sus datos personales.

7.2... de forma inteligible y **de fácil acceso y utilizando un lenguaje claro y sencillo**.

7.3... **Será tan fácil retirar el consentimiento como darlo**.

Artículo 8 Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, la edad que se establece para el **consentimiento lícito son los 16. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.**

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

Listado de Derechos del Interesado

Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado

Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

Artículo 15 Derecho de acceso del interesado

Artículo 16 Derecho de rectificación

Artículo 17 Derecho de supresión («el derecho al olvido»)

Artículo 18 Derecho a la limitación del tratamiento

Artículo 19 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

Artículo 20 Derecho a la portabilidad de los datos

Artículo 21 Derecho de oposición

Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles

Información de acceso

ASECCIÓN 2. Información y acceso a los datos personales

Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

… el responsable del tratamiento... le facilitará toda la información indicada a continuación:

a) **la identidad y los datos de contacto del responsable** y, en su caso, de su representante;

b) **los datos de contacto del delegado de protección de datos**, en su caso;

c) l**os fines del tratamiento a que se destinan los datos personales** y la base jurídica del tratamiento.

d) **cuando el tratamiento se base en** el artículo 6, apartado 1, letra f), los **intereses legítimos** del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la **intención del responsable de transferir datos personales a un tercer país u organización internacional** y la existencia o ausencia de una decisión de adecuación de la Comisión,

...

Derechos de los interesados

LOPD/RDLOPD

- **A**CCESO.
- **R**ECTIFICACIÓN.
- **C**ANCELACIÓN.
- **O**POSICIÓN.

- Revocación del consentimiento

GDPR

Artículo 15 Derecho de acceso del interesado

SECCIÓN 3. Rectificación y supresión

Artículo 16 Derecho de rectificación

Artículo 17 Derecho de supresión («el derecho al olvido»)

Artículo 18 Derecho a la limitación del tratamiento

Artículo 19 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

Artículo 20 Derecho a la portabilidad de los datos

SECCIÓN 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21 Derecho de oposición

biantik

PIA, Privacy by Design y la violación de la seguridad...

Los Responsables como los Encargados, deberán probar el cumplimiento respecto a la identificación del riesgo relacionado con el tratamiento. Para ello, deberán hacer una evaluación en términos de origen, naturaleza, probabilidad y gravedad así como la identificación de buenas prácticas para mitigar el riesgo pudiendo materializarse en códigos de conducta aprobados, certificaciones aprobadas, etc.

Cualquier violación de la seguridad en materia de datos personales, el Responsable deberá notificarlo a la autoridad de control competente, a menos que pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación entrañe un riesgo para los derechos y las libertades de la persona.

Incidencias (Procedimiento de Respuesta ante Incidencias) según RDLOPD:

Notificación.

Registrar soluciones o desenlaces.

¿Que se considera incidencia?

Recuperaciones de datos de copias de respaldo

Virus detectados

Cualquier elemento que afecte a seguridad de ficheros

biantik

LinkedIn

Aviso de filtración de datos

Puede que hayas oído recientemente noticias referentes a un problema de seguridad en LinkedIn. Queremos asegurarnos de que cuentas con los hechos de lo sucedido, qué tipo de información resultó afectada y qué pasos estamos dando para protegerte.

Qué sucedió

El 17 de mayo de 2016 llegó a nuestro conocimiento que datos robados de LinkedIn en 2012 se habían publicado en Internet. No fue un fallo de seguridad o acto pirateo nuevo. Tomamos inmediatamente medidas para invalidar las contraseñas de todas las cuentas de LinkedIn que creíamos que podrían estar en peligro. Dichas cuentas se habían creado antes del fallo de seguridad de 2012 y no habían restablecido sus contraseñas desde entonces.

Qué información resultó afectada

Direcciones de correo electrónico de los miembros, contraseñas codificadas (hashed) y números de identificación de miembro de LinkedIn (un código interno que LinkedIn asigna a cada perfil de miembro) de 2012.

Para más información

Si tienes cualquier pregunta, no dudes en comunicarte con nuestro equipo de Confianza y seguridad: tns-help@linkedin.com. Para más información, visita nuestro blog oficial.

Qué medidas estamos tomando

Hemos invalidado las contraseñas de todas las cuentas de LinkedIn creadas antes del fallo de seguridad de 2012 que no habían sido restablecidas desde el incidente. Además, hemos creado herramientas automatizadas para tratar de identificar y bloquear cualquier actividad sospechosa que pudiera afectar a las cuentas de LinkedIn. Estamos asimismo colaborando con las fuerzas del orden.

LinkedIn ha tomado medidas importantes para fortalecer la seguridad de las cuentas desde 2012. Por ejemplo, ahora utilizamos criptografía con sal para almacenar las contraseñas y ofrecemos a los miembros la opción de aplicar la verificación en dos pasos como medida de seguridad adicional.

Qué puedes hacer

Tenemos varios equipos dedicados a asegurarnos de que la información que los miembros proporcionan a LinkedIn esté segura. Al mismo tiempo, siempre sugerimos que nuestros miembros visiten el Centro de seguridad para informarse de cómo habilitar la verificación en dos pasos y crear contraseñas fuertes para que sus cuentas permanezcan lo más seguras posible. Te recomendamos que cambies la contraseña de LinkedIn a menudo y, si empleas la misma contraseña o una parecida en otros sitios web, que establezcas nuevas contraseñas para esas cuentas.

biantik

CONCEPTOS A TENER EN CUENTA

Integridad

Disponibilidad

Riesgo

Amenaza

Confidencialidad

Vulnerabilidad

Denegación del Servicio

Identificación

Autenticación

Tipos de Ataques

Incidencias

Más términos en: http://bit.ly/V8oHKg

Certificaciones

Artículo 57 y 58: funciones y poderes respectivamente

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

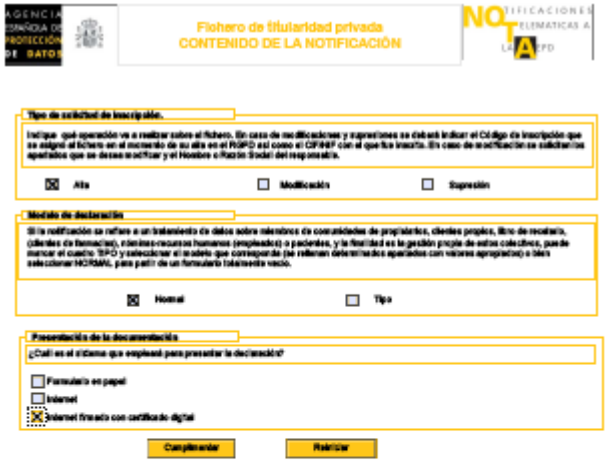
Artículo 42 Certificación

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

INSCRIPCIÓN FICHEROS | LOPD/RDLOPD

DOCUMENTACIÓN:

- **Inscripción de Ficheros:** clasificación y detección de los ficheros a notificar y a inscribir en el registro de la AGPD cuya titular será la entidad auditada. Para ello se descargará previamente el formulario nota y se elegirá entre privada y pública dependiendo del tipo de entidad auditada, para el envió del formulario, optaremos por:
  - **Normal.** - **Tipo.**
- Internet firmado con certificado digital.
- Internet.
- Formulario en papel.
- Sede electrónica.



Inscripción Ficheros | GDPR

Artículo 30 Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de Datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

biantik

Inscripción Ficheros | GDPR

Artículo 30 Registro de las actividades de tratamiento

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable

…Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, **el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.**

5. **Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas**, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, **o incluya categorías especiales de datos personales indicadas en el artículo 9...**

Derecho al Olvido hasta ahora

Derecho al Olvido, los datos ya no son necesarios, se retira el consentimiento, ha expirado plazo conservación y no existe otra base jurídica tratamiento, interesado se opone, el tratamiento de datos no es conforme **RGLPD** al por cualquier otro motivo.

FORMULARIOA

Jarri beharko dugun informazioa URL bakoitzaren azpikaldean: *En el ejercicio de mi derecho al olvido plasmado y reconocido en la sentencia del TJUE y dado que la información a la que se hace referencia en la actualidad ya no es noticia y son excesivos en relación con estos fines y el tiempo transcurrido. Por el presente escrito solicito a Google que deje de indexar y vincular mi nombre y los consiguientes datos personales al introducirlos en el motor de búsqueda de Google a la/ las siguiente/s URL/s:*

Derecho al Olvido, los datos ya no son necesarios, se retira el consentimiento, ha expirado plazo conservación y no existe otra base jurídica tratamiento, interesado se opone, el tratamiento de datos no es conforme **RGLPD** al por cualquier otro motivo.

FORMULARIOA

Jarri beharko dugun informazioa URL bakoitzaren azpikaldean: *En el ejercicio de mi derecho al olvido plasmado y reconocido en la sentencia del TJUE y dado que la información a la que se hace referencia en la actualidad ya no es noticia y son excesivos en relación con estos fines y el tiempo transcurrido. Por el presente escrito solicito a Google que deje de indexar y vincular mi nombre y los consiguientes datos personales al introducirlos en el motor de búsqueda de Google a la/ las siguiente/s URL/s:*

- Si no está satisfecho con la decisión que ha tomado Google, tiene derecho a denunciar el caso ante la autoridad competente en materia de derechos de protección de datos de su país. Si decide hacerlo, puede incluir el número de referencia de xxxxxxxxxxxxx y una copia de la confirmación de envío del formulario que nos ha enviado.
- También puede enviar su solicitud de retirada de contenido directamente al webmaster responsable del sitio web en cuestión. El webmaster puede retirar el contenido del sitio web o bloquearlo para que no aparezca en los motores de búsqueda. En la página https://support.google.com/websearch/answer/9109?hl=es dispone de información sobre cómo ponerse en contacto con el webmaster de un sitio.

Derecho al Olvido

- Si responsable los publicó: Informar a terceros requerimiento de borrado de copias, réplicas o enlaces, salvo necesarios:
- Ejercicio libertad de expresión, interés publico en el ámbito de la salud pública, investigación histórica, estadística y científica, cumplimiento de una obligación legal de conservar los datos personales.

  Ezezko erantzuna: Hola, Gracias por su mensaje: Tras examinar su solicitud, hemos decidido no llevar a cabo ninguna acción en este momento. En relación con las siguientes URL:
- En este caso, parece que las URL que ha identificado incluían información acerca de usted que es relevante para asuntos de interés público. Por tanto, concluimos que la referencia a este documento en nuestros resultados de búsqueda está justificada por el interés público en tener acceso a él.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Derecho al Olvido GDPR

Artículo 17 Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), LICITUD...

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, (Derecho de Oposición) y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (niños).

Derecho al Olvido GDPR

2. **Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales**, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) 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;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Mila esker!

¡Gracias!

www.biantik.coop

biantik@biantik.coop

Ion Turrillas Sabalza

ion.turrillas@biantik.coop

@jonturrillas

http://www.linkedin.com/in/jonturrillas

09/06/2016