



REGLAMENTO  
GENERAL DE  
PROTECCIÓN DE DATOS

2016

ECIJA

# Report -Reglamento General de Protección de Datos

ANTECEDENTES

P.4

---

PRINCIPALES NOVEDADES

P.7

---

MEDIDAS Y PLAZOS

P.12

SOLUCIONES ECIJA

P.15

---

PREGUNTAS FRECUENTES

P.16

---

Área de  
Privacidad  
y  
Protección  
de Datos

[www.ecija.com](http://www.ecija.com)





## Report - Reglamento General de Protección de Datos

La aprobación el 14 de abril de 2016 del Reglamento General de Protección de Datos, pone fin al camino emprendido años atrás para homogeneizar las diferentes regulaciones sobre datos personales a nivel europeo, unificando su normativa en todos los Estados miembros. Un hito que supone para las empresas el reto de adaptarse a las obligaciones y exigencias establecidas por la norma europea, una oportunidad competitiva para operar en el mercado global.

Es por tanto esencial que todas las organizaciones (empresas e instituciones, entre otras) que traten datos personales, tengan presente cuáles son las nuevas reglas que serán de aplicación en la protección de los derechos de los ciudadanos, así como cuáles son las oportunidades competitivas que esta nueva normativa pone a su disposición para competir en un mercado global.

Así, el conocimiento de dichas reglas se convierte en un pilar fundamental para las organizaciones, aportando seguridad jurídica a sus operaciones, aportando valor a los clientes y usuarios desde el respeto a sus derechos y privacidad, reduciendo riesgos sancionatorios y reputacionales, optimizando sus recursos y procesos en relación con el tratamiento de datos personales.

Desde el Área de Privacidad y Protección de Datos de ECIJA hemos preparado este Report con el objetivo de analizar las novedades que el Reglamento implica para empresas y particulares en su actividad cotidiana, facilitando su adaptación a las nuevas reglas de juego, fomentando la cultura del cumplimiento y el respeto a la privacidad y la protección de las personas.

**Área de Privacidad y Protección de Datos ECIJA**



Firma líder en asesoramiento en Derecho de  
Tecnología, Medios y Telecomunicaciones

## 01. ANTECEDENTES

El derecho a la protección de datos se encuentra configurado como un derecho fundamental de las personas, tal y como recogen las diferentes Constituciones nacionales. Un derecho que tiene el origen de su protección en el Convenio 108 y que se consolidaría con la 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.

El imparable avance de la tecnología, junto con las exigencias marcadas por los propios acontecimientos, han puesto de manifiesto una y otra vez la necesidad de avanzar en una regulación unificada del derecho a la protección de los datos. Un Mercado único digital, pone de manifiesto la necesidad de adoptar normas que garanticen la protección de las personas, y que permitan el avance de nuevos modelos de negocio basado en las posibilidades que aportan las nuevas tecnologías.

Así, a principios de 2012 comenzaba un largo camino hasta su aprobación el Reglamento Europeo de Protección de Datos. Una norma que pretende reconocer la mayoría de edad de empresas e instituciones en el tratamiento de los datos personales, dotando a Europa de una regulación pionera y acorde al siglo XXI.

Determinadas obligaciones formales, tales como la inscripción de ficheros que reconocía la Directiva, dan paso a la adopción de garantías y cautelas por los responsables de ficheros y tratamientos, desde la concepción de la privacidad como valor en el diseño de los productos.

Una conciliación de la protección del derecho de las personas y el desarrollo de la economía digital, orientada al reconocimiento de la autonomía de las personas a decidir sobre sus datos personales, bajo una nuevas reglas donde prime la transparencia. Una norma del presente preparada para una sociedad del futuro.

## 02. PRINCIPALES NOVEDADES

La aprobación del Reglamento Europeo de Protección de Datos supone la incorporación a nuestro ordenamiento de nuevos aspectos jurídicos que, sin duda, afectaran de forma directa a empresas, consumidores y usuarios. En particular, el objetivo principal de este reglamento es proporcionar un mayor control a los interesados sobre de su información privada y, así, adaptar la legislación europea, en mayor medida, a la sociedad de la información. Una necesaria armonización a nivel europeo de las exigencias y requisitos en materia de protección de datos.

### Principales novedades para las organizaciones:



Principio de **RESPONSABILIDAD**. Las organizaciones tendrán que implementar medidas que permitan acreditar que están adoptando todas las medidas necesarias para realizar un correcto tratamiento de los datos personales de los que dispone.



Obligación, en determinados casos, de realizar **EVALUACIONES DE IMPACTO** que determinen los riesgos específicos que supone tratar ciertos datos de carácter personal.



Avance en la adopción de principios de protección de datos por **DEFECTO Y DESDE EL DISEÑO**, orientados a adoptar la cultura de la privacidad en el seno de la organización y garantizar la privacidad de las personas.



Posibilidad de que el responsable del fichero pueda establecer un **CANON** teniendo en cuentas los costes administrativos asociados a la contestación de los ejercicios del derecho de acceso por las personas.



Designación de un Delegado de Protección de Datos (DPO).



Comunicación de las **BRECHAS DE SEGURIDAD** a autoridades de control y a los afectados, tan pronto sean conocidas, estableciéndose el plazo máximo de 72 horas tras su conocimiento.



**VENTANILLA ÚNICA**. Las empresas tendrán como interlocutora a una sola autoridad de control. Se estima que esto supondrá un ahorro de 2300 millones euros al año que dispone.



Normas específicas que favorecerán la **INNOVACIÓN**. Las normas establecerán que las garantías de protección de datos se incorporen en los productos y servicios desde sus primeras fases de desarrollo (priva-



# Principales novedades para las organizaciones



Avance en la adopción de **GARANTÍAS** sobre el tratamiento de los datos personales y las personas y entidades que participan del mismos, en este sentido la selección de encargados de tratamiento que aporten garantía a dichos tratamientos de datos jugaran un papel relevante.



Principio de **TRANSPARENCIA** en el tratamiento de los datos personales y el principio de **ACCOUNTABILITY**. Simplificación de los avisos legales y cláusulas facilitando su comprensión por las personas cuyos datos van a ser tratados.



Eliminación de la actual obligación de **INSCRIPCIÓN DE LOS FICHEROS** en la Agencias y Autoridades de Protección de Datos, sustituyendo dicha obligación por el control interno, inventario, de los ficheros, datos tratados, flujos de tratamiento realizados por las empresas





"Una norma del presente preparada para una sociedad del futuro"

## Principales novedades para particulares:



Mayor **TRANSPARENCIA** e **INFORMACIÓN** a los ciudadanos por parte de las organizaciones al tratar sus datos personales, facilitando una mayor información sobre los periodos de conservación de los mismos, las finalidades de tratamiento y las entidades que van a participar en él.



Consolidación del **DERECHO AL OLVIDO**. Los interesados podrán revocar el consentimiento prestado para el tratamiento de sus datos personales en cualquier momento, pudiendo exigir la supresión y eliminación de los datos que consideren oportunos en redes sociales o buscadores de internet. Del mismo modo, se refuerza la protección sobre los menores en este asunto.

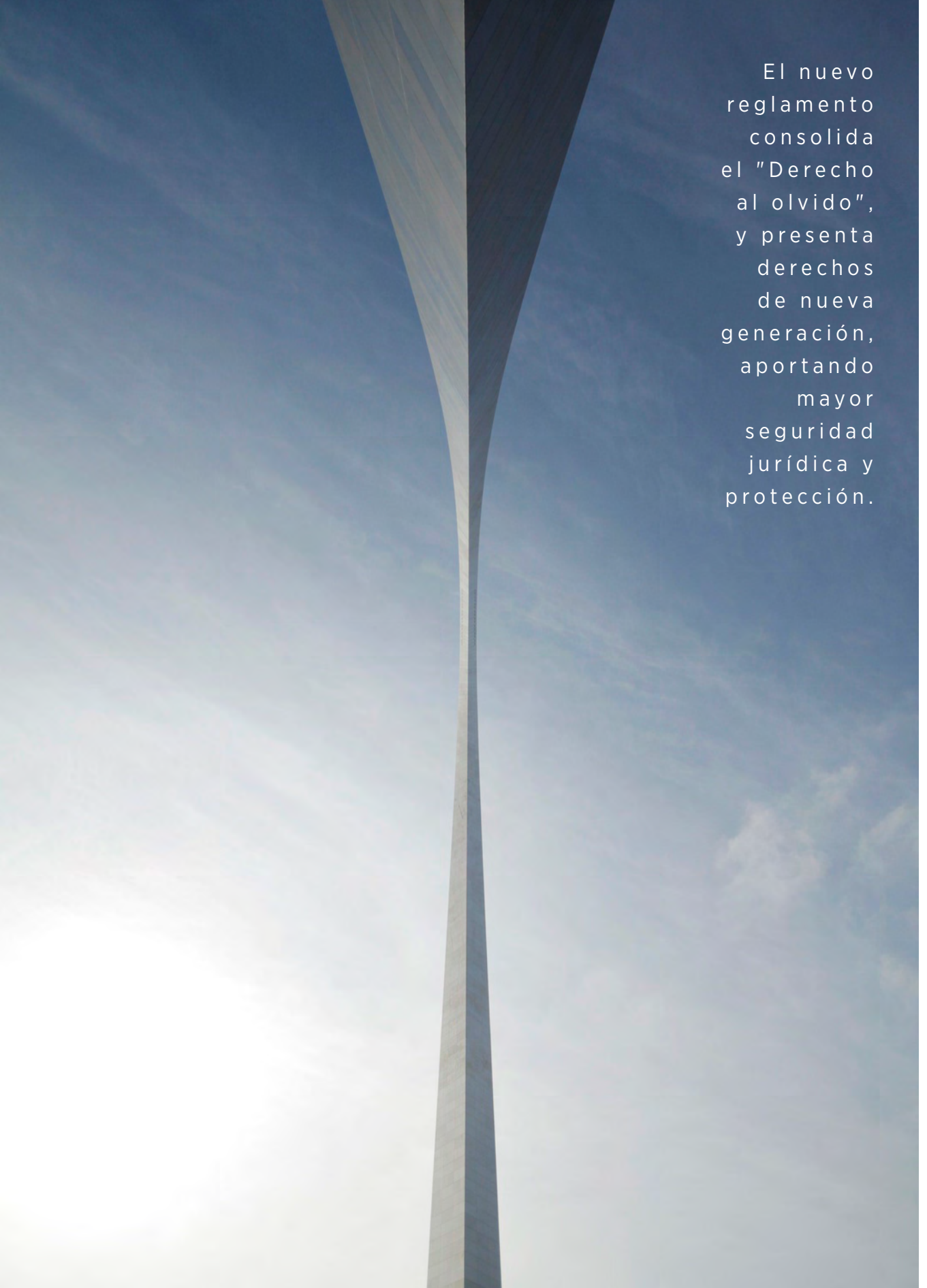


Derecho a la **PORTABILIDAD DE LOS DATOS**. Se permitirá transferir los datos personales del interesado de manera más sencilla de un proveedor de servicios en Internet a otro, siempre dando el control al ciudadano para que decida sobre su tratamiento final.

Transparencia  
e información

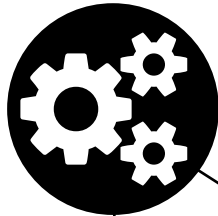
Derecho al olvido  
y protección  
menores

Portabilidad de  
los datos



El nuevo  
reglamento  
consolida  
el "Derecho  
al olvido",  
y presenta  
derechos  
de nueva  
generación,  
aportando  
mayor  
seguridad  
jurídica y  
protección.

## Otras novedades a tener en cuenta:



### Tipos de datos:

Ampliación de los datos considerados como especialmente protegidos, con la inclusión de los datos genéticos y biométricos.

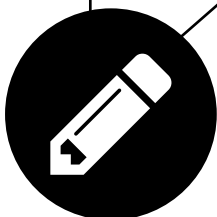
### Garantías:

Establecimiento de garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fuera de la Unión Europea.



### Sello de cumplimiento:

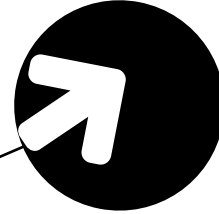
Establecimiento de sellos de cumplimiento (Sello Europeo)





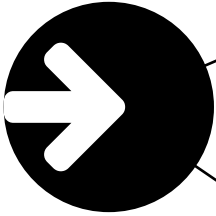
## Denuncias:

Posibilidad de presentar denuncias a través de asociaciones de usuarios y reconocimiento de la posibilidad de exigir daños y perjuicios, así como indemnizaciones derivadas del tratamiento ilícito de los datos personales.



## Sanciones:

Las cuantías de las sanciones asociadas al incumplimiento de la norma, pudiendo llegar a los 20 millones de euros o el 4% de la facturación general anual.





REGISTRO

---

DPO

---

CONSENTIMIENTO

---

RESPONSABILIDAD

---

EVALUACIONES

---

SEGURIDAD

## 03. MEDIDAS Y PLAZOS:

El Reglamento Europeo de Protección de Datos de carácter personal establece un período transitorio de dos años a partir de su entrada en vigor, esto es, 20 días desde su publicación en el Diario Oficial de la Unión Europea.

Las disposiciones contenidas en el Reglamento son directamente aplicables a todos los Estados Miembros.



¿Qué cambios  
afectan  
en mayor  
medida a las  
organizaciones?

# 1. Registro

Se deberá llevar un registro interno y por escrito de las diferentes actividades desarrolladas en la empresa que conlleven un tratamiento de datos, ya que se elimina la necesidad de inscribir ante el Registro de la Agencia Española de Protección de Datos los distintos ficheros responsabilidad de las empresas

# 2. DPO

Se deberá designar un Delegado de protección de datos siempre y cuando:

- El tratamiento lo lleve a cabo una autoridad pública.
- Efectúen un tratamiento de datos las actividades principales que consista en operaciones que requieran de un seguimiento regular y se realicen a gran escala.
- Se efectúen tratamientos sobre categorías de datos especialmente protegidas a gran escala.

# 3. Consentimiento

El consentimiento para poder tratar datos de carácter personal ha de ser inequívoco, libre y revocable y deberá darse mediante un acto afirmativo claro.



## 4. Responsabilidad

Responsabilidad de quienes efectúen los tratamientos de datos a fin de demostrar que se cumplen con las exigencias contempladas en el Reglamento. Se trata de una responsabilidad proactiva, es decir, se debe demostrar que la empresa ha materializado dichas exigencias a través por ejemplo de políticas, procedimientos, controles, etc.

## 5. Evaluaciones de impacto

Previamente a efectuar determinados tratamientos (elaboración de perfiles, tratamiento a gran escala de las categorías especiales de datos, entre otros) las empresas deberán elaborar una evaluación de impacto, en la que se analicen los posibles riesgos que pudiera conllevar el nuevo tratamiento sobre los datos que se va a efectuar.

## 6. Privacy by design / by default

Protección de datos desde el diseño y por defecto: las empresas que tratan datos personales deberán tener en cuenta todas las disposiciones de la normativa que puedan afectarles antes de efectuar del tratamiento, por ejemplo, antes de desarrollar una herramienta informática y aplicarán las medidas técnicas y organizativas que correspondan. Asimismo, se deberán tratar los datos imprescindibles para llevar a cabo un determinado tratamiento, garantizando de tal forma que, por defecto, solo serán objeto de tratamiento aquellos datos que sean necesarios para los fines específicos del tratamiento.



¿Qué cambios  
afectan  
en mayor  
medida a las  
organizaciones?



## 04. SOLUCIONES ECIJA

Desde ECIJA ofrecemos asesoramiento especializado basado en un conocimiento exhaustivo de la normativa y las exigencias de los diferentes modelos de negocio y sectores, facilitando el acercamiento a las normas y su aplicación teniendo en cuenta la propia idiosincrasia empresarial, desde la conciliación de la tecnología y el derecho.

Durante el proceso de adecuación a la nueva norma europea, ECIJA ofrece, entre otros, los siguientes servicios:

- Adopción de procedimientos o redefinición de políticas corporativas.
- Asesoramiento en la realización de evaluaciones de impacto / riesgos, e implementación de procesos privacy by design o privacy by default.
- Formación de empleados sobre el cumplimiento de la nueva normativa.
- Realización de auditorías de cumplimiento
- Elaboración y definición de mapas de riesgos conforme al sector de actividad.
- Asesoramiento en la definición de las funciones y los quehaceres del Delegado de Protección de Datos.

Además, junto con el equipo de profesionales de la Firma, ECIJA cuenta con diferentes herramientas propias de gestión de la normativa de protección de datos, que le facilitan funcionalidades adaptadas a los requisitos y exigencias del Reglamento Europeo de Protección de Datos. Una solución de cumplimiento normativo para mejorar la eficacia de la gestión y facilitar el principio de accountability (acreditación del cumplimiento).

## 05. PREGUNTAS FRECUENTES

**P: ¿Cuándo entrará en vigor el Reglamento Europeo de Protección de Datos?**

La entrada en vigor del Reglamento tendrá lugar a los 20 días de su publicación en el Diario Oficial de la Unión Europea. Sin embargo, sus disposiciones no resultarán de aplicación hasta transcurridos dos años a partir de la fecha de su publicación en el Diario Oficial de la Unión Europea.

**P: ¿Cuál será el ámbito de aplicación del nuevo Reglamento?**

El ámbito de aplicación del Reglamento comprende aquellos tratamientos de datos realizados en el marco de la actividad de responsables del tratamiento establecidos en la UE.

**P: ¿Se modifica el régimen del deber de información y consentimiento del titular de los datos?**

Sí. El responsable del tratamiento deberá facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento de datos leal y transparente, teniendo en cuenta las circunstancias en que se produce el tratamiento y el origen de los datos.

**P: ¿Qué novedades introduce la nueva configuración del “derecho al olvido”?**

En particular, los interesados tienen reconocido el derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados, si los interesados han retirado su consentimiento para el tratamiento, o se oponen libremente al tratamiento.

---

### El nuevo Reglamento será aplicable a partir del próximo año 2018

---

**P: ¿Cuáles son las sanciones que enfrentarán empresas y organizaciones por el incumplimiento del nuevo régimen de Protección de Datos?**

Las multas se incrementarán con respecto a las establecidas en la Ley Orgánica de Protección de datos.

- a) Multas económicas de hasta 10.000.000 de euros o hasta 2% del volumen de negocios mundial del ejercicio económico anterior; o
- b) Multas económicas de hasta 20.000.000 EUR o hasta 4% del volumen de negocios mundial.

**P: ¿Qué deberán tener en cuenta las empresas y organizaciones con respecto al tratamiento de datos de carácter personal?**

El nuevo Reglamento incorpora la exigencia para las empresas y organizaciones de actuar de conformidad con el “principio de responsabilidad proactiva”. Esto se traduce en la realización periódica de evaluaciones de impacto, siempre que el tratamiento de los datos entrañe un riesgo para los derechos y libertades de los titulares de los datos, y la adopción, con carácter previo al tratamiento y durante el mismo, de aquellas medidas técnicas y organizativas que resulten precisas para determinar los riesgos que puede conllevar un determinado tratamiento de datos.





**P: ¿Es obligatorio el nombramiento de un Data Protection Officer?**

Las empresas y organizaciones estarán obligadas al nombramiento de un DPO (ya sea internamente o externalizándolo en un tercero) cuando las actividades principales del responsable consistan en operaciones de tratamiento a gran escala que, o bien se refieran al tratamiento de categorías de datos especialmente protegidos, o que requieran un seguimiento continuado de los interesados.

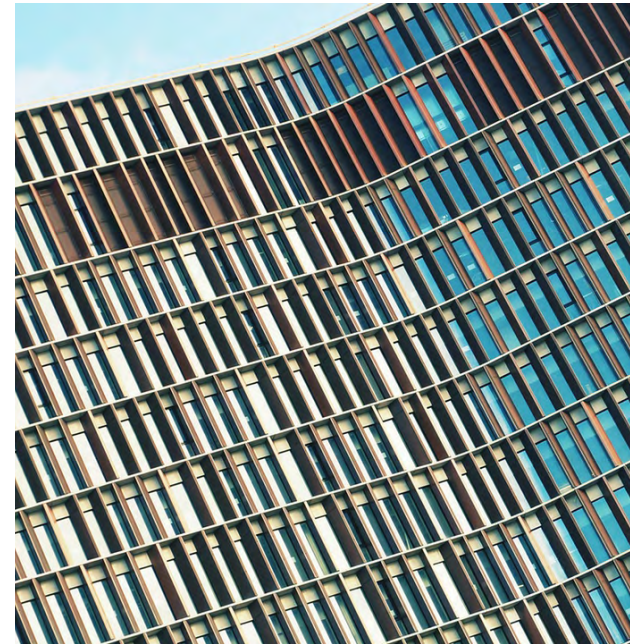
**P: ¿Las empresas y organizaciones deberán seguir declarando ficheros ante la Agencia Española de Protección de Datos?**

No. El Reglamento enfoca las obligaciones de registro desde un punto de vista interno con respecto al entorno organizativo de las empresas y organizaciones. Éstas deberán cumplimentar formularios de registro de tratamiento a nivel interno por escrito, cuyo contenido será muy similar al del actual Fichero Nota. Este registro a nivel interno deberá encontrarse disponible a solicitud de la Agencia Española de Protección de Datos, que podrá disponer de él en el ejercicio de su facultad inspectora.

**P: ¿Qué autoridad de control nacional será competente para atender cuántas cuestiones se deriven de la actuación de una empresa u organización que opere en más de un Estado Miembro de la UE?**

Resultará de aplicación el principio de “ventanilla única”, en virtud del cual, en determinados casos, la Autoridad de Control del lugar en que se encuentre el establecimiento principal de un responsable o encargado del tratamiento dentro de la Unión Europea actúe como autoridad de control principal para los tratamientos de datos transfronterizos.

**Se elimina la obligación de empresas e instituciones de declarar ficheros ante la Agencia Española de Protección de Datos**



**P: ¿Las empresas y organizaciones tendrán la obligación de notificar una brecha de seguridad o una fuga de información a la Agencia Española de Protección de Datos y a los interesados?**

Sí. En el caso de que exista una vulneración de datos que pueda perjudicar los derechos de los titulares de los datos, el Responsable del Tratamiento tendrá la obligación de notificarlo a la Agencia Española de Protección de Datos en el plazo de setenta y dos (72) horas, así como notificarlo a los interesados a la mayor brevedad posible. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

**P: ¿Cómo deberán proceder las empresas y organizaciones hasta el momento en que resulten de aplicación las disposiciones del nuevo Reglamento Europeo de Protección de Datos?**

El Reglamento impone numerosas obligaciones que requerirán significativos esfuerzos de carácter organizativo, técnico, económico y humano. Por ello, una completa implementación de las obligaciones del Reglamento implica necesariamente que las organizaciones se familiaricen con el contenido del Reglamento e inicien el diseño de los planes para su implantación desde este mismo momento de su aprobación.

# Contacto

Alonso Hurtado  
Socio

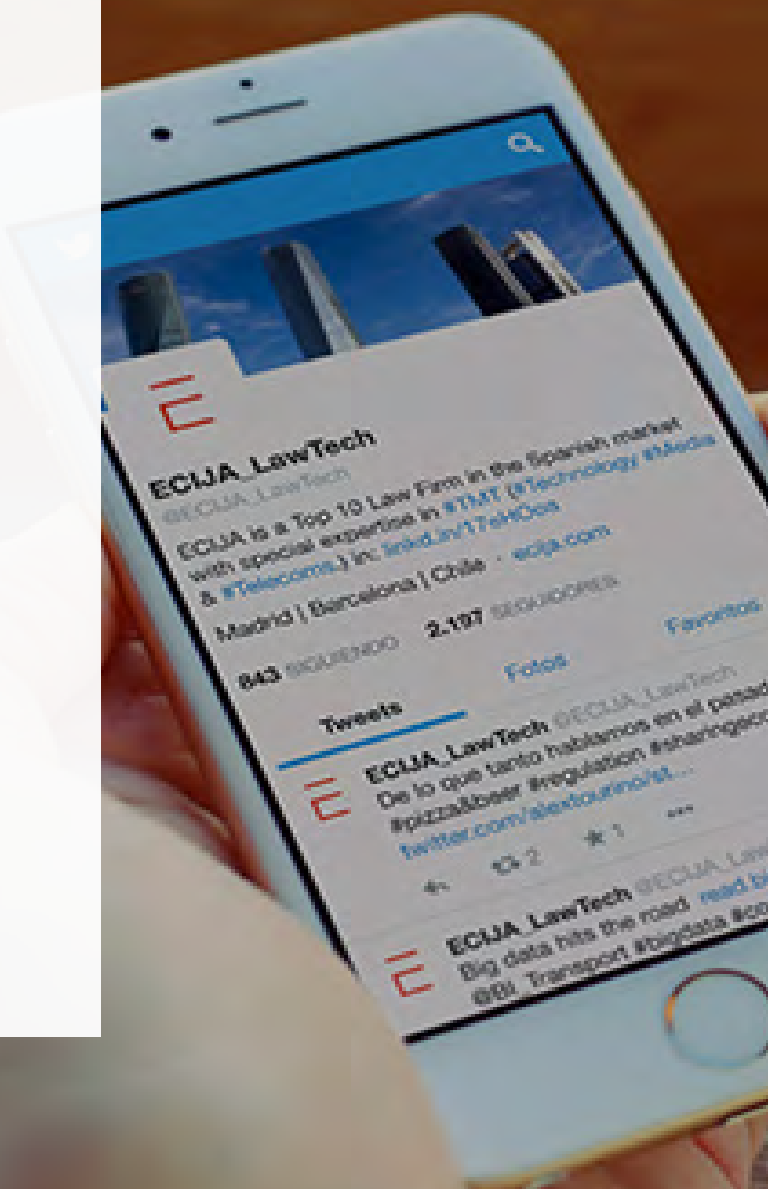
alhurtado@ecija.com  
91.781.61.60

---

Daniel López  
Asociado senior  
dlopez@ecija.com  
91.781.61.60

---

María González  
Asociada senior  
mgonzalezm@ecija.com  
91.781.61.60



Este report sido elaborado por el área de Privacidad y Protección de Datos de ECIJA



[www.ecija.com](http://www.ecija.com)