



Comisión
Europea

ESTADO DE
LA UNIÓN
2018



Proteger los datos personales de los ciudadanos europeos en las elecciones

#SOTEU

12 de septiembre de 2018

«Quiero que el próximo mes de mayo los europeos puedan tomar sus decisiones políticas en unas elecciones europeas justas, seguras y transparentes. En nuestro mundo en línea, el riesgo de intromisión y manipulación nunca ha sido tan elevado. Ha llegado el momento de que nuestras normas electorales se pongan a la altura de la era digital para proteger la democracia europea».

Jean-Claude Juncker, 12 de septiembre de 2018



Los partidos políticos utilizan cada vez más los datos personales para dirigirse a los ciudadanos a través de las redes sociales durante los períodos electorales. Las revelaciones de Cambridge Analytica ponen de manifiesto el riesgo que pueden suponer para el proceso electoral las tecnologías modernas. La Comisión ha establecido hoy directrices sobre la manera en que las normas de la UE deben utilizarse para abordar esta cuestión y garantizar la equidad del proceso electoral, especialmente en la antesala de las elecciones al Parlamento Europeo de 2019.

El Reglamento general de protección de datos de la UE, que entró en vigor en mayo de 2018, establece normas claras sobre la manera en que todos los agentes implicados en las elecciones deben desempeñar su papel y cumplir las nuevas normas de protección de datos.



Obligaciones de los partidos políticos y las fundaciones políticas

Los partidos políticos y las fundaciones políticas son responsables del tratamiento de los datos, ya que deciden la razón por la que se tratan los datos personales y la manera de hacerlo.

QUÉ DEBEN HACER:

- ☁ Elegir la **base jurídica adecuada** para el tratamiento de los datos de las personas y prestar atención a las condiciones específicas para el tratamiento de los datos sensibles.
- ☁ Asegurarse de que los sistemas que utilizan son **seguros** y, si se produce una violación de los datos, informar al respecto sin demora.
- ☁ Informar a las personas al inicio del tratamiento de sus datos y también cuando estos se recaben de terceros.
- ☁ Asegurarse de que los datos tratados son exactos, especialmente cuando se recopilan datos de diversas fuentes.
- ☁ Si recurren a los servicios de un **tercero** (por ejemplo, a una empresa de análisis de datos), comprobar si los datos recibidos del tercero se han obtenido legalmente.

QUÉ NO DEBEN HACER:

- ☁ No deben utilizar datos de personas si estas los han cedido para un **fin** que no esté relacionado con el contexto electoral específico.
- ☁ No deben dar derechos de **acceso** sin restricciones a los datos que se tengan de las personas. Se debe comprobar quién tiene acceso a los datos dentro de la organización y para qué fines legítimos.





Empresas de análisis de datos e intermediarios de datos

Las empresas de análisis de datos y los intermediarios de datos son, bien responsables o bien encargados del tratamiento de los datos, dependiendo del grado de control que tengan sobre el tratamiento. Por ejemplo, se considera que una empresa de análisis de datos que trata los datos de personas siguiendo instrucciones de un partido político es la encargada del tratamiento de los datos.

QUÉ DEBEN HACER:

- ☁ Elegir la **base jurídica adecuada** para tratar los datos de las personas.
El texto que figura a continuación solo es válido si la empresa de análisis de datos o el intermediario de datos es el responsable del tratamiento de los datos.
- ☁ Si tratan **datos sensibles** (por ejemplo, el origen étnico), deben contar con el consentimiento expreso de la persona o aplicar otras excepciones previstas por el Reglamento general de protección de datos.
- ☁ Asegurarse de que los sistemas que utilizan son **seguros** y, si se produce una violación de los datos, informar al respecto sin demora.
- ☁ Si combinan diferentes **conjuntos de datos** sobre las personas, asegurarse de que esto se hace con exactitud y de forma legal.
El último punto solo es válido si la empresa de análisis de datos o el intermediario de datos es el encargado del tratamiento de los datos.
- ☁ Ayudar a los **terceros** con los que se trabaje (por ejemplo, los partidos políticos) cuando precisen su ayuda, por ejemplo, para elaborar una evaluación de impacto de la protección de datos.

QUÉ NO DEBEN HACER:

- ☁ No deben utilizar datos de personas si estas los han cedido para un **fin** que no esté relacionado con el contexto electoral específico.
- ☁ No deben eludir la obligación de informar a las personas sobre todos los fines del tratamiento, especialmente cuando se trate de una venta a un tercero (por ejemplo, a un partido político).



Autoridades electorales nacionales

Las autoridades electorales nacionales son **responsables del tratamiento de los datos**, ya que controlan el censo electoral.

QUÉ DEBEN HACER:

- Llevar a cabo una **evaluación de impacto** de protección de datos para evaluar el riesgo antes de empezar a tratar los datos de las personas.
- Por lo general, la **base jurídica** para tratar los datos de las personas será el cumplimiento de una obligación legal o la realización de una tarea de interés público con arreglo a la legislación.



Plataformas de redes sociales

Las plataformas de las redes sociales son responsables del tratamiento de los datos, porque en sus plataformas tiene lugar el tratamiento de los datos de las personas.

QUÉ DEBEN HACER:

- ☁ Elegir la **base jurídica adecuada** para tratar los datos de las personas.
- ☁ Si tratan **datos sensibles** (por ejemplo, el origen étnico), deben contar con el consentimiento expreso de la persona o aplicar otras excepciones previstas por el Reglamento general de protección de datos.
- ☁ Dar a las personas los **controles y opciones de configuración** necesarios para que puedan ejercer sus derechos de manera efectiva, por ejemplo cuando soliciten la rectificación o la supresión de sus datos.
- ☁ Asegurarse de que los sistemas que utilizan son **seguros** y, si se produce una violación de los datos, informar al respecto sin demora.

QUÉ NO DEBEN HACER:

- ☁ No deben compartir los datos con **terceros**, por ejemplo con una empresa de análisis de datos, a menos que los usuarios hayan dado su consentimiento expreso.
- ☁ Si comparten los datos de sus usuarios con terceros, deben especificarlo claramente en las condiciones de uso de la plataforma.