PODEMOS

MANUAL DEL PERSONAL DE PODEMOS CON ACCESO A DATOS DE CARÁCTER PERSONAL

INDICE

1. La protección de datos de carácter personal

El objeto de este manual es explicar de forma sencilla las funciones y obligaciones que deben conocer y cumplir todos los usuarios de los ficheros de datos personales de Podemos Partido Político.

La protección de los datos de carácter personal de los ciudadanos se encuentra regulada en la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** (a la que denominaremos LOPD) y en una serie de normas que la desarrollan y la complementan, principalmente el Real Decreto 1720/2007, de 21 de diciembre, que aprobó el **Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**, donde se regulan las medidas de seguridad que deben implantar los responsables de los tratamientos o los ficheros y los encargados del tratamiento.

Estas normas garantizan una serie de derechos a las personas físicas titulares de datos, como el derecho a ser informado sobre la incorporación de sus datos en un fichero, el derecho a acceder a sus datos, el derecho a rectificarlos o a cancelarlos cuando lo desee y el derecho a que no sean cedidos a terceras personas sin su consentimiento.

Y para proteger estos derechos la ley establece una serie de medidas de obligado cumplimiento para todas las personas y entidades que, en el ejercicio de una actividad, registren datos de carácter personal en un soporte físico susceptible de tratamiento.

La importancia de conocer y cumplir con todas las obligaciones que se incluyen en este manual deriva de que la protección de los datos personales es un derecho fundamental reconocido en la Constitución Española y está protegido con sanciones económicas muy elevadas para los casos de incumplimiento.

Por ejemplo, la vulneración del deber de guardar secreto acerca del tratamiento de los datos que tienen las personas que intervengan en cualquier fase del tratamiento de los datos se considera una infracción grave y puede ser sancionada con una multa de 40.000 a 300.000 euros.

Por eso es muy importante extremar las precauciones en materia de secreto y de seguridad informática, cumpliendo fielmente y con responsabilidad todas las obligaciones que se indican a continuación.

La Agencia Española de Protección de Datos es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales, actuando para ello con plena independencia de las Administraciones Públicas.

2. Definiciones

Parar cumplir con las obligaciones legales es necesario en primer lugar tener una noción básica de las definiciones utilizadas por la ley.

DATO DE CARÁCTER PERSONAL: cualquier información concerniente a personas físicas identificadas o identificables.

Es decir, cualquier información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables a través del dato.

FICHERO: todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso, ya sea en formato papel o en formato electrónico.

Un fichero es cualquier sistema o conjunto de datos que esté organizado mediante algún criterio, por ejemplo, una aplicación de datos, una tabla de texto, una hoja de cálculo o un archivo con fichas de papel.

FICHERO DE CARÁCTER TEMPORAL: aquellos en los que se almacenan datos de carácter personal derivados del cumplimiento de una necesidad puntual y siempre que no sea superior a un mes, los cuales deben ser destruidos una vez haya finalizado la necesidad que motivó su creación.

TRATAMIENTO DE DATOS: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias de datos.

El tratamiento es precisamente una de las funciones que realizarán los usuarios, cualquier operación que se haga con los datos (grabarlos, consultarlos, enviarlos, modificarlos, conservarlos, etc.).

RESPONSABLE DE FICHERO O TRATAMIENTO: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

El responsable del fichero normalmente coincidirá con la organización: empresa, institución, profesional …. Es aquel que tiene que cumplir con la mayoría de la obligaciones en protección de datos siendo el responsable de las sanciones que se impongan derivadas de su incumplimiento.

AFECTADO O INTERESADO: persona física titular de los datos.

Es la persona cuyos datos están incluidos en el fichero (inscritos, colaboradores, talentos, empleados, etc.)

ENCARGADO DE TRATAMIENTO: persona física o jurídica que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero o tratamiento.

El encargado del tratamiento es cualquier persona o empresa que, en virtud de un contrato, presta un servicio al responsable del fichero y que para ello tiene que acceder a los datos del responsable.

El responsable del fichero puede tener varios encargados de tratamiento, internos o externos a la organización.

Podemos tiene un encargado interno de tratamiento y varios encargados externos de tratamiento, como las empresas que prestan el servicio de alojamiento de ficheros.

No se consideran encargados del tratamiento a los empleados o a los colaboradores que tengan acceso a los datos en virtud de una relación laboral o de colaboración con el responsable del fichero o del encargado del tratamiento.

USUARIO: persona autorizada a acceder a datos personales o sistemas de tratamiento de datos.

El usuario es cualquier persona que accede a los datos de la organización, con diferentes perfiles de acceso, debidamente autorizado a ello mediante la suscripción del correspondiente documento de acceso y confidencialidad.

CONSENTIMIENTO DEL INTERESADO: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen.

CESIÓN O COMUNICACIÓN DE DATOS: toda revelación de datos realizada a una persona distinta del interesado.

3. Funciones y obligaciones de los usuarios

Todo el personal de Podemos, ya sean empleados o colaboradores, que tengan autorizado el acceso a los ficheros de datos personales debe cumplir las siguientes obligaciones:

A) Obligaciones generales

1. **Guardar secreto sobre cualquier dato de carácter personal** inscrito en los ficheros de Podemos a los que pudiera tener acceso, ya sea autorizado o no, comprometiéndose a no comunicarlos ni cederlos a terceros.

2. **Guardar secreto sobre toda la información confidencial de Podemos**, en especial sobre su organización interna, su infraestructura tecnológica, los nombres de usuario y claves de acceso.

3. **Mantener el compromiso de secreto y confidencialidad de forma indefinida** tras finalizar la relación laboral o de colaboración con Podemos o la autorización de acceso que le fue concedida.

4. **Acceder únicamente a los ficheros y datos para los que tenga autorización de acceso y que sean estrictamente necesarios** para realizar las funciones que tenga encomendadas, cumpliendo en todo momento la legislación vigente sobre protección de datos de carácter personal y los reglamentos internos y manuales de usuario de Podemos que le sean entregados.

5. **No realizar copias de la información confidencial y de los datos de carácter personal de los ficheros**, en cualquier medio o soporte, físico o digital.

6. **No trasladar documentos o soportes digitales que contengan datos de carácter personal** de los ficheros de Podemos o cualquier información confidencial fuera de los locales de Podemos ni de su lugar de trabajo particular sin la debida autorización del responsable de seguridad.

7. **Guardar en lugar seguro todos los soportes físicos** que contengan datos de carácter personal y no desvelar la ubicación de los mismos a terceras personas.

8. **Borrar y destruir todos los ficheros de carácter temporal** una vez que no sean necesarios para los fines que motivaron su creación.

9. **No introducir, modificar, extraer o anular datos** en los ficheros de Podemos sin la debida autorización del responsable del fichero o del encargado del tratamiento.

10. **Comunicar al responsable de seguridad las incidencias de seguridad** de las que tenga conocimiento, de acuerdo con el procedimiento de notificación establecido por el responsable de seguridad.

B) Obligaciones específicas respecto a ficheros automatizados.

11. **Usar los sistemas informáticos y tratar los datos personales siguiendo las instrucciones facilitadas por el responsable del fichero, el encargado del tratamiento y el responsable del servicio.**

12. **Cumplir las medidas de seguridad dictadas por el responsable de seguridad** y todas las que sean necesarias, tanto en los locales de Podemos como en su lugar de trabajo personal.

13. **No utilizar las contraseñas de otros usuarios.** Está totalmente prohibido utilizar identificadores y contraseñas de otros usuarios para acceder al sistema.

14. **No anotar las contraseñas** de acceso en lugares fácilmente accesibles o visibles por terceros y modificarlas a petición del sistema o del responsable de seguridad.

15. **No comunicar los nombres de usuario o las contraseñas a terceras personas**.

16. **No desvelar la ubicación de los servidores** internos ni las URL de acceso a los ficheros almacenados en servidores externos.

17. **Cerrar o bloquear las sesiones al finalizar la utilización de la base de datos**.

18. **No acceder a las bases de datos utilizando redes informáticas públicas o desde ordenadores o equipos de uso público o de terceras personas**.

19. **No modificar la ubicación informática ni los nombres de los ficheros de datos de carácter personal**.

20. **No instalar aplicaciones informáticas** en los servidores centrales ni en los equipos informáticos de Podemos salvo autorización del responsable de seguridad.

21. **No realizar copias de los archivos ni de los datos en el disco duro de equipos móviles**, como ordenadores portátiles, tabletas o teléfonos aunque sean temporales, ya sean equipos propios como de Podemos.

22. **Si el usuario utiliza su propio equipo informático** para el acceso a los ficheros de datos personales deberá disponer de las medidas de seguridad establecidas por el responsable de seguridad, en especial, la utilización de contraseñas de arranque, de cortafuegos y de sistemas de protección contra virus informáticos.

C) Obligaciones específicas respecto a ficheros no automatizados

23. **Custodiar las llaves de acceso** a los locales, despacho, armarios, archivadores u otros elementos que contengan ficheros no automatizados de carácter personal, poniendo en conocimiento del responsable de seguridad cualquier hecho que pueda haber comprometido esa custodia.

24. **Supervisar el cierre de las puertas de acceso** al finalizar la jornada de trabajo.

25. **Guardar en lugar seguro los soportes físicos y documentos** que contengan información con datos de carácter personal cuando no sean utilizados, sobretodo al finalizar la jornada laboral.

26. **No dejar documentos que contengan datos de carácter personal sobre las mesas** de trabajo una vez finalizada la jornada laboral.

27. **Controlar las impresoras, fotocopiadoras y equipos de fax** para evitar el descuido de documentos que contengan datos personales.

4. Gestión de incidencias.

Incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Son ejemplos de incidencias de seguridad:

- *olvido de contraseña,*
- *bloqueo de cuenta por reiteración de intentos de conexión fallidos,*
- *borrado accidental de datos,*
- *descubrimiento de virus informáticos,*
- *detección de accesos no autorizados al ordenador personal,*
- *robo o pérdida de llaves de locales en los que se guarden datos personales, etc.*

El usuario deberá comunicar inmediatamente al responsable de seguridad y al encargado interno de tratamiento cualquier incidencia de seguridad de la que tenga conocimiento, por correo electrónico a web@podemos.info y a lopd@podemos.info

EQUIPO DE PODEMOS LOPD