DECRETO

Expediente nº: 1705/2025
Resolución con número y fecha establecidos al margen
Procedimiento: Cumplimiento de Obligaciones en Protección de Datos de Carácter Personal

HECHOS Y FUNDAMENTOS DE DERECHO

RESOLUCIÓN POR LA QUE SE APRUEBA EL DOCUMENTO DE POLÍTICA DE PROTECCIÓN DE DATOS EN EL AYUNTAMIENTO DE SANTIPONCE

Con motivo de la aprobación y entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119 /1, 04-05-2016) (en adelante, RGPD), se ha proporcionado un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa.

En tal sentido, el artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», que exige una actitud consciente, diligente y proactiva por parte de las Administraciones Públicas frente a todos los tratamientos de datos personales que lleven a cabo.

En tal sentido, el Ayuntamiento de Santiponce aboga por una política proactiva de cumplimiento, en aras de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

En el documento de Política de Protección de Datos, se identifican los datos concretos del responsable del tratamiento, asumiendo el compromiso por parte de este Ayuntamiento, de garantizar el cumplimiento de la mencionada normativa, que, en España, se ha desarrollado a través de la Ley Orgánica 3 /2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Asimismo, se alude a la figura del Delegado de Protección de Datos, acreditando la necesaria existencia de éste dentro de la entidad, conforme al artículo 37.1.a) del RGPD. A lo largo del texto del documento, se justifica la detección de no ser necesaria la evaluación de impacto, se expone la evaluación de riesgo, y se crea el registro de acciones informativas y formativas para el personal de la entidad.

En virtud de cuanto antecede, y con el fin de dar cumplimiento a la normativa anteriormente citada, en uso de las atribuciones conferidas por el artículo 21.1. s) de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local,
RESUELVO:

Vista la propuesta de resolución PR/2025/1697 de 7 de octubre de 2025.

RESOLUCIÓN

PRIMERO. Aprobar el Documento de Política de Protección de Datos en el Ayuntamiento de Santiponce, que se anexa a esta Resolución, asumiendo el compromiso de dar cumplimiento al mismo, con el fin de garantizar el amparo del derecho a la protección de datos de carácter personal, en los términos que establece el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

SEGUNDO. Dar traslado de esta Resolución al personal de la entidad, así como a los Concejales-Delegados de Servicios de este Ayuntamiento, para su conocimiento y cumplimiento.

TERCERO. Publicar la presente Resolución, junto con el documento aprobado, en el tablón de anuncios de la sede electrónica, y de la página web municipal, para la garantía de la transparencia pública del mismo.

DOCUMENTO FIRMADO ELECTRÓNICAMENTE

Documento de Política de Protección de Datos

POLÍTICA DE PROTECCIÓN DE DATOS

CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679
Y LA NORMATIVA ESPAÑOLA DE PROTECCIÓN DE DATOS

audidat
PROTECCIÓN DE DATOS

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

a) Nombre y datos de contacto del responsable del tratamiento:

- Denominación social / Nombre y apellidos: Ayuntamiento de Santiponce
- CIF/NIF: P4108900D
- Actividad: Otras actividades
- Teléfono de contacto: 657817849
- Domicilio social: Calle Arroyo, 41970 - Santiponce (Sevilla)
- Domicilio a efecto de notificaciones: Calle Arroyo, 41970 - Santiponce (Sevilla)
- Dirección electrónica de contacto: adlsantiponce@gmail.com
- Página web (URL): http://santiponce.es

b) Nombre y datos de contacto del corresponsable del tratamiento:

- No existe la figura del corresponsable del tratamiento

c) Nombre y datos de contacto del representante del responsable:

- El representante del tratamiento está establecido en el territorio de la Unión Europea

d) Nombre y datos de contacto del delegado de protección de datos:

- Nombre y apellidos: Mª del Pilar Hernandez
- Dirección electrónica de contacto:pilarsecretaria@santiponce.es

I. OBJETO DEL DOCUMENTO.

La Agencia Española de Protección de Datos plasmó, en su Plan Estratégico 2015-2019, su voluntad de que los responsables del tratamiento alcancen un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (en adelante, RGPD), proporciona un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa.

En tal sentido, el artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento será responsable del cumplimiento (y capaz de demostrarlo) de los siguientes principios relativos al tratamiento:

- Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

- Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

- Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

- Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

- Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de

investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

- Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

En síntesis, el principio de «responsabilidad proactiva» exige una actitud consciente, diligente y proactiva por parte de las Administraciones Públicas frente a todos los tratamientos de datos personales que lleven a cabo.

En tal sentido, el Ayuntamiento de Santiponce aboga por una política proactiva de cumplimiento, en pos de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

En su consecuencia, el presente documento se elabora con el objeto de establecer la Política de Ayuntamiento de Santiponce en relación con el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y en la normativa española de protección de datos de carácter personal (Ley Orgánica, sus normas de desarrollo y la legislación sectorial específica).

II. COMPROMISO DEL AYUNTAMIENTO CON LA PROTECCIÓN DE DATOS.

El Ayuntamiento de Santiponce (en adelante, el responsable del tratamiento), asume la máxima responsabilidad y compromiso con el establecimiento, implementación y mantenimiento de la presente Política de Protección de Datos, garantizando la mejora continua del responsable del tratamiento con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y de la normativa española de protección de datos de carácter personal (Ley Orgánica, legislación sectorial específica y sus normas de desarrollo).

La Política de Protección de Datos de Ayuntamiento de Santiponce descansa en el principio de responsabilidad proactiva, según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

En tal sentido, el responsable del tratamiento se regirá por los siguientes principios que deben servir a todo su personal como guía y marco de referencia en el tratamiento de datos personales:

1. Protección de datos desde el diseño: el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento.

2. Protección de datos por defecto: el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

3. Protección de datos en el ciclo de vida de la información: las medidas que garanticen la protección de los datos personales serán aplicables durante el ciclo completo de la vida de la información.

4. Licitud, lealtad y transparencia: los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

5. Limitación de la finalidad: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

6. Minimización de datos: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

7. Exactitud: los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

8. Limitación del plazo de conservación: los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

9. Integridad y confidencialidad: los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

10. Información y formación: una de las claves para garantizar la protección de los datos personales es la formación e información que se facilite al personal involucrado en el tratamiento de los mismos. Durante el ciclo de vida de la información, todo el personal con acceso a los datos será convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la normativa de protección de datos.

La Política de Protección de Datos de Ayuntamiento de Santiponce es comunicada a todo el personal del responsable del tratamiento y puesta a disposición de todas las partes interesadas.

En su consecuencia, la presente Política de Protección de Datos involucra a todo el personal del responsable del tratamiento, que debe conocerla y asumirla, considerándola como propia, siendo cada miembro responsable de aplicarla y de verificar las normas de protección de datos aplicables a su actividad, así como identificar y aportar las oportunidades de mejora que considere oportunas con el objetivo de alcanzar la excelencia en relación con su cumplimiento.

Esta Política será revisada por el Ayuntamiento de Santiponce, tantas veces como se considere necesario, para adecuarse, en todo momento, a las disposiciones vigentes en materia de protección de datos de carácter personal.

En Santiponce, a la fecha de la firma electrónica,

Fdo. D. Juan José Ortega Gordón
Representante legal del Ayuntamiento de Santiponce

III. NECESIDAD DE DISPONER DE UN DELEGADO DE PROTECCIÓN DE DATOS.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), determina en su artículo 37.1.a) que deberá nombrarse un Delegado de Protección de Datos en caso de que:

> "*el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial*".

Atendiendo a lo dispuesto en el referido precepto legal, se detecta la necesidad de que Ayuntamiento de Santiponce disponga de un Delegado de Protección de Datos.

IV. NECESIDAD DE REALIZAR UNA EVALUACIÓN DE IMPACTO.

NO se detecta la necesidad de realizar una evaluación de impacto.

Esto es debido a que **no** se da ninguno de los siguientes supuestos:

- El responsable realiza una **evaluación sistemática y exhaustiva** de aspectos personales de personas físicas que se basa en un tratamiento automatizado, como la **elaboración de perfiles**, y sobre cuya base se toman decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

- El responsable realiza tratamientos **a gran escala** de **categorías especiales** de datos personales:
  - Datos personales que revelen el **origen étnico o racial.**
  - Datos personales que revelen las **opiniones políticas.**
  - Datos personales que revelen las **convicciones religiosas o filosóficas.**
  - Datos personales que revelen la **afiliación sindical.**
  - Datos **genéticos.**
  - Datos **biométricos** dirigidos a identificar de manera unívoca a personas físicas.
  - Datos relativos a la **salud** (física o mental).
  - Datos relativos a la **vida sexual** o la **orientación sexual** de personas físicas.
  - Datos relativos a **condenas e infracciones penales**, así como a procedimientos y medidas cautelares y de seguridad conexas.

- El responsable realiza una **observación sistemática a gran escala** de una **zona de acceso público.**

Concepto de "sistemático"
El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:
- *Que se produce de acuerdo con un sistema;*
- *Preestablecido, organizado o metódico;*
- *Que tiene lugar como parte de un plan general de recogida de datos;*
- *Llevado a cabo como parte de una estrategia.*

V. EVALUACIÓN DEL RIESGO.

Determinación del riesgo

La mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan.

De tal modo, el responsable del tratamiento está obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el citado Reglamento, con la Ley Orgánica, sus normas de desarrollo y la legislación sectorial específica, incluida la eficacia de dichas medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

En su consecuencia, el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En tal sentido, los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos siguientes:

- En los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;

- En los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales;

- En los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;

- En los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales;

- En los casos en los que se traten datos personales de personas vulnerables, en particular niños;

- En los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

Determinación del riesgo de las operaciones de tratamiento

La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. Así, el riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un **escaso riesgo**, **riesgo (riesgo estándar)** o un **alto riesgo**.

A los efectos de la presente política de protección de datos, deberá considerarse que las operaciones del tratamiento suponen un **alto riesgo** para los derechos y libertades de las personas físicas en los siguientes supuestos:

1. Cuando el tratamiento pueda generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

2. Cuando el tratamiento pueda privar a los afectados de sus derechos y libertades o pueda impedirles el ejercicio del control sobre sus datos personales.

3. Cuando se produzca el tratamiento **no meramente incidental o accesorio** de las siguientes categorías de datos:

    - Datos personales que revelen el origen étnico o racial.
    - Datos personales que revelen las opiniones políticas.
    - Datos personales que revelen las convicciones religiosas o filosóficas.
    - Datos personales que revelen la afiliación sindical.
    - Datos genéticos.
    - Datos biométricos dirigidos a identificar de manera unívoca a una persona física.
    - Datos relativos a la salud.

- Datos relativos a la vida sexual o la orientación sexual de una persona física.
- Datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas.

4. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

5. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

6. Cuando se produzca un tratamiento masivo que afecte a un gran número de afectados o implique la recogida de una gran cantidad de datos personales.

7. Cuando los datos de carácter personal fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección. En tal sentido, se considera que tienen un nivel adecuado de protección los siguientes Estados:

    - Los Estados del **Espacio Económico Europeo (EEE)**:

        - Estados de la Unión Europea.
        - Islandia.
        - Liechtenstein.
        - Noruega.

    - **Suiza**. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.

    - **Canadá**. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

    - **Argentina**. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.

    - **Guernsey**. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.

    - **Isla de Man**. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.

    - **Jersey**. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.

- **Islas Feroe**. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
- **Andorra**. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
- **Israel**. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
- **Uruguay**. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
- **Nueva Zelanda**. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
- **Japón.** Decisión de 23 de enero de 2019.
- **Reino Unido.** Decisión de 28 de junio de 2021**.**
- **República de Corea.** Decisión de 17 de diciembre de 2021.
- **EU- USA Data Privacy Framework** Decisión de 10 de julio de 2023. relación de las entidades certificadas**:** **https://www.dataprivacyframework.gov/s/**

8. Otros supuestos de riesgo en base a la actividad del responsable del tratamiento.

VI. REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS.

La Política de Protección de Datos de Ayuntamiento de Santiponce descansa en el principio de responsabilidad proactiva, según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

En tal sentido, el responsable del tratamiento se rige, entre otros, por el principio de información y formación, según el cual una de las claves para garantizar la protección de los datos personales es la formación e información que se facilite al personal involucrado en el tratamiento de los mismos, educando a los empleados en la denominada cultura de la protección de datos.

En su consecuencia, todo el personal de la entidad con acceso a los datos será convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la normativa de protección de datos, recibiendo el apropiado conocimiento, capacitación y actualizaciones regulares de la Política de Protección de Datos de Ayuntamiento de Santiponce.

En relación con la metodología de las acciones informativas y formativas, se recomienda la combinación de diferentes metodologías para una mejor asimilación de los conocimientos por parte de los participantes, citando a modo de ejemplo las siguientes:

- Exposición de contenidos o clase magistral: El docente explica los contenidos de forma teórica con ayuda de recursos como son presentaciones de PowerPoint.

- Simulaciones o estudio del caso: El docente propone situaciones a resolver por parte de los participantes, que le permiten asimilar mejor los conocimientos adquiridos.

- Dinámicas de grupo: Con el fin de activar la interacción entre los participantes y el docente.

En relación con el personal docente, se recomienda acudir a profesionales de la protección de datos y de la privacidad con experiencia docente previa. Esta función puede recaer sobre el propio delegado de protección de datos de la entidad responsable del tratamiento, en el caso de que se hubiese designado como tal. Asimismo, al finalizar la acción formativa, se aconseja la realización de pruebas de evaluación de conocimientos a los participantes.

Con la finalidad de la gestión de control interno del cumplimiento del principio de información y formación en el seno de la entidad, se ha elaborado un “Registro de acciones formativas e informativas” para el personal en materia de protección de datos.

REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS		
REF. ACCIÓN INFORMATIVA Y/O FORMATIVA N.º 1		
Identificación de la acción informativa y/o formativa		
Denominación de la acción		
Nombre de la entidad impartidora		
Datos de contacto de la entidad impartidora		
Caracterización de la acción informativa y/o formativa		
Modalidad de formación	☐	Formación presencial
	☐	Teleformación
Objetivos de la acción formativa		
Perfil de las personas participantes		
Duración de la acción formativa		
Descripción abreviada del programa y contenidos de la acción formativa		
Metodología de la acción formativa		
Personal docente		
Recursos didácticos utilizados en la formación		
Evaluación de la formación		

REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS		
REF. ACCIÓN INFORMATIVA Y/O FORMATIVA N.º 2		
Identificación de la acción informativa y/o formativa		
Denominación de la acción		
Nombre de la entidad impartidora		
Datos de contacto de la entidad impartidora		
Caracterización de la acción informativa y/o formativa		
Modalidad de formación	☐	Formación presencial
	☐	Teleformación
Objetivos de la acción formativa		
Perfil de las personas participantes		
Duración de la acción formativa		
Descripción abreviada del programa y contenidos de la acción formativa		
Metodología de la acción formativa		
Personal docente		
Recursos didácticos utilizados en la formación		
Evaluación de la formación		