Procedimiento de Evaluaciones de Impacto relativas a Protección de Datos (EIPD)

Protección de datos

Procedimiento de Evaluaciones de Impacto

Procedimiento de Evaluaciones de Impacto del Ayuntamiento de Bolaños de Calatrava, para cumplir con el artículo 35 del Reglamento General de Protección de Datos (RGPD).

Información del documento

Control de versiones

Versión	Fecha	Descripción de cambios
V 1.0	08/07/2022	Versión inicial del documento

Propiedad del documento

Propietario: Ayuntamiento de Bolaños de Calatrava

Elaborado: GRUPO CIES

INDICE

1 Objeto

El objeto del presente documento es establecer el procedimiento a seguir en el Ayuntamiento de Bolaños de Calatrava , en adelante, el Ayuntamiento, para cumplir con lo establecido en el artículo 35 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), según el cual, el Ayuntamiento deberá realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de las personas afectadas.

2 Alcance del Documento

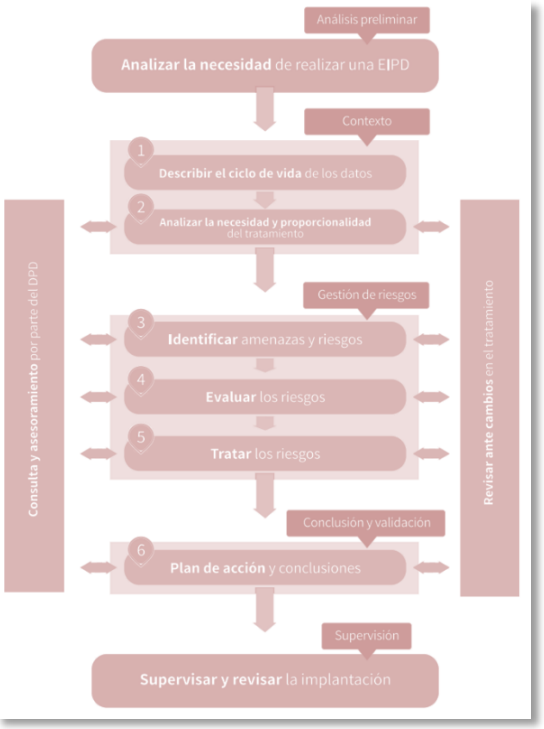
El presente procedimiento se aplicará a los nuevos tratamientos que se inicien en el Ayuntamiento y aquellos que habiendo estado sujetos a la realización de una Evaluación de Impacto en Protección de Datos (EIPD) hayan sido modificados y deban ser revisados.

3 Contenido y fases de una EIPD

La Evaluación de Impacto sobre Protección de Datos (EIPD) consistirá en la elaboración de un informe en el que conste como mínimo los siguientes contenidos sobre el tratamiento analizado:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés público perseguido por el Ayuntamiento.
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
c) una evaluación de los riesgos para los derechos y libertades de las personas afectadas.
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de las personas afectadas.

Las etapas para la ejecución de un EIPD:



No obstante, si del análisis preliminar se determina que no es necesario realizar la EIPD se archivará la EIPD, salvo que el Ayuntamiento decida continuar con su ejecución. En todo caso se dejará constancia de la realización del Análisis de la necesidad llevado a cabo.

4 El análisis previo

Cuando sea probable que un tipo de tratamiento realizado en el Ayuntamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Ayuntamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

El artículo 35 del RGPD, viene a considerar los supuestos en los que se puede prever con mayor detalle, cuando es requisito el proceso de evaluación de impacto, considerando y en orden de prelación:

a) El tratamiento está incluido en una lista derivada del artículo 35.5 RGPD (NO requiere EIPD) Lista publicada por la Agencia Española de Protección de Datos (AEPD).

b) El tratamiento está incluido en una lista derivada del artículo 35.4 RGPD (SÍ requiere EIPD). El tratamiento se encuentra incluido en varios supuestos de los publicados por la AEPD.

c) El tratamiento está incluido en alguno de los supuestos previstos en el 35.3 del RGPD (SÍ requiere EIPD).

    a. Situaciones en las que NO es necesario hacer una EIPD

Si el tratamiento está incluido en una lista derivada del artículo 35.5 RGPD (NO requiere EIPD) según la lista publicada por la Agencia Española de Protección de Datos (AEPD). Esta lista* se basa en el

documento WP 2481 y complementa su criterio con el objeto de ayudar a los responsables a determinar qué tratamientos no requieren de una EIPD.

- Directrices o decisiones AEPD: Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.
- Códigos de conducta: Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.
- Obligación legal e interés público: Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

(*) de esta lista se ha omitido aquellos supuestos no aplicables al Ayuntamiento como responsable del tratamiento.

Si el tratamiento analizado se ajusta a alguna de estas circunstancias no será preciso la realización de una EIPD independientemente que se cumpla alguno de los requisitos establecidos para la realización de una EIPD.

4.1 Situaciones en las que es necesario realizar una EIPD

La EIPD será tal necesaria tal y como establece el artículo 35.3 del RGPD en los siguientes casos:

- Elaboración de perfiles: evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamientos a gran escala: tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.
- Seguimiento y control de personas: observación sistemática a gran escala de una zona de acceso público (videovigilancia a gran escala, vigilancia electrónica, biometría, técnicas genéticas, geolocalización, RFID, etc.)

Si el tratamiento analizado se ajusta a alguna de estas circunstancias será preciso la realización de una EIPD.

Supuestos basados en el artículo 35.4 RGPD (varios supuestos de los publicados por la AEPD):

Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 *"Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD"*, para ello se determinará si el tratamiento analizado cumple con al menos dos de los siguientes supuestos:

- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc. (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables, por ejemplo, escucha activa para conocer preferencia de usuarios de RRSS o internet).
- Tratamientos que impliquen el uso de categorías especiales de datos, relativos a condenas o infracciones penales o aquellos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de dato. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- Tratamientos que impliquen el uso de datos genéticos para cualquier fin.
- Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "*Directrices sobre los delegados de protección de datos (DPD)*" del Grupo de Trabajo del Artículo 29.
- Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.
- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

- Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
- Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

Si se cumplen 2 o más de estas circunstancias será preciso la realización de una EIPD.

5 Procedimiento para la realización de una EIPD

Todas las áreas/departamentos del Ayuntamiento que deseen iniciar un nuevo tratamiento, o deseen modificar sustancialmente una actividad de tratamiento en curso, deberán solicitar asesoramiento a la persona designada como delegado/a de Protección de Datos a través del correo electrónico: dpd@bolanosdecalatrava.es, previo al inicio del tratamiento o de la modificación y de la inscripción del mismo en el Registro de Actividades de Tratamiento (RAT) según el procedimiento establecido a tal efecto.

La persona designada como delegado/a de Protección de Datos analizará cada propuesta de nuevo tratamiento o modificación de este y colaborará y asesorará al Ayuntamiento en la determinación de la necesidad o no de realizar una EIPD y en su realización, si procediera, así como modificación del RAT o inclusión en el mismo de una nueva actividad de tratamiento, si fuera preciso.

Será la persona designada como delegado/a de Protección de Datos quien documentará el análisis preliminar en donde se determinará la necesidad o no de realizar una EIPD. Para ello se ayudará del CUESTIONARIO EVALUACIÓN PREVIA EIPD. El resultado obtenido en dicho análisis preliminar será comunicado a las áreas correspondientes con anterioridad al inicio del tratamiento.

Se utilizará el enfoque metodológico descrito en el presente procedimiento tanto para la realización del análisis previo, como la gestión de los riesgos y su posterior tratamiento.

6 Fases de la EIPD. Consulta a los interesados y Análisis Preliminar

b. Consulta a los interesados

Una de las opciones que ofrece el RGPD, independientemente del análisis posterior sobre la necesidad o no de realizar una EIPD, es recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o de la seguridad de las operaciones de tratamiento. Las áreas involucradas deberán consultar a la persona designada como Delegado/a de Protección de Datos sobre si es conveniente la realización de dicha consulta y, caso afirmativo, la forma de llevarla a cabo.

c. Evaluación de la necesidad de realizar una EIPD

Cuando sea probable que un tipo de tratamiento realizado en el Ayuntamiento en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Ayuntamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

El artículo 35.3 del RGPD, establece aquellos casos particulares en los que se requerirá una EIPD:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
b) Tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales.
c) Observación sistemática a gran escala de una zona de acceso público.

Así mismo, los art. 35.4 y 35.5 del RGPD otorgan potestad a las Autoridades de Control para la publicación de listados de actividades y operaciones de tratamiento que pudieran requerir o no la realización de una EIPD. Las exigencias contempladas en los precitados artículos están desarrolladas en el CUESTIONARIO EVALUACIÓN PREVIA EIPD del presente procedimiento, cuestionario que se debe tener como referencia por parte del Ayuntamiento para evaluar y documentar la necesidad o no de realizar una EIPD.

7 Fases de la EIPD. Contexto

a. Descripción del ciclo de vida de los datos

La EIPD conlleva tener un conocimiento muy claro del contexto y de los procesos a analizar. Como punto de partida, es necesario conocer en detalle todo el ciclo de vida y el flujo de los datos personales a través de este y todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin.

b. Análisis de la necesidad y proporcionalidad del tratamiento

Se deben analizar detalladamente todas las finalidades para las cuales se recaban los datos personales para determinar la necesidad de llevar a cabo el tratamiento y evaluar si la finalidad que se persigue se puede conseguir por otros medios menos invasivas para la privacidad de aquellas personas cuyos datos serán tratados.

Para poder evaluar la necesidad y la proporcionalidad del tratamiento y poder comprobar si dicho tratamiento supone una medida restrictiva del derecho fundamental a la protección de datos, debe superar los tres puntos del denominado juicio de proporcionalidad:

a) Juicio de idoneidad ¿se consigue el objetivo propuesto?

b) Juicio de necesidad: ¿existen otras alternativas para conseguir la misma finalidad?
c) Juicio de proporcionalidad en sentido estricto: ¿son mayores las ventajas que los perjuicios?

8 Fases de la EIPD. Gestión de Riesgos

La gestión de riesgos es el proceso de identificar, analizar y valorar la probabilidad e impacto derivados de la posibilidad de que se materialice un riesgo con el objetivo de establecer las acciones preventivas, correctivas y reductivas que permitan minimizar el nivel de exposición al riesgo. La fase de gestión de riesgos se divide en las siguientes etapas:

a) Identificación de los riesgos. Se trata de analizar los potenciales escenarios de riesgos (exposición a amenazas) a los que pueden estar expuestos los datos de carácter personal, prestando especial atención a la confidencialidad, integridad y disponibilidad.
b) Evaluación de los riesgos.
   Se debe valorar y estimar la probabilidad de ocurrencia y el impacto para los derechos y libertades del interesado, de que un riesgo se materialice. Se recomienda utilizar los criterios definidos en la metodología Magerit, alineada con el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad, las recomendaciones descritas en la Guía CCN-STIC 882 sobre análisis de riesgos en Entidades Locales y la Guía de Análisis de Riesgos publicada por la Agencia Española de Protección de Datos.
c) Tratamiento de los riesgos. En esta última etapa para gestionar los riesgos se deben establecer las medidas necesarias para reducir su nivel de exposición hasta alcanzar un nivel aceptable. Para ello existen cuatro tipos de medidas diferentes:
   1. Reducir el riesgo mediante controles que reduzcan la probabilidad y/o el impacto.
   2. Retener el riesgo si es considerado un riesgo aceptable por el Ayuntamiento.
   3. Transferir el riesgo mediante, por ejemplo, una aseguradora que afronte las posibles consecuencias materiales.
   4. Anulación del riesgo: abandonar la actividad de tratamiento si el riesgo no es asumible por el Ayuntamiento.

9 Fases de la EIPD. Informe, plan de acción y conclusiones

Una vez completados los pasos anteriores, se procederá a elaborar un Plan de acción, que se incluirá en el informe final de la EIPD, en donde se definirán todas las iniciativas que se deben llevar a cabo para implantar los controles que ayuden a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable de forma que se garanticen los derechos y libertades de las personas físicas en lo que se refiere al tratamiento de sus datos personales.

La conclusión de la EIPD se basará en el nivel de riesgo residual obtenido durante la fase de gestión de riesgos. Si la conclusión de la EIPD es favorable, la actividad de tratamiento se puede llevar a cabo, siempre y cuando las medidas de control incluidas en el plan de acción hayan sido implantadas.

Si la conclusión de la EIPD no es favorable, deberá contemplarse la implementación de medidas adicionales. Si no fuese posible, el tratamiento no podría llevarse a cabo y sería necesario elevar una consulta a las Autoridades de Control.

10 Fases de la EIPD. Consulta previa a la Autoridad de Control

Si una vez realizada la EIPD el resultado muestra que el tratamiento sigue teniendo un alto riesgo para los derechos y libertades de las personas afectadas, aún tras aplicar las garantías, medidas de seguridad y mecanismos de protección razonables en cuanto a técnica disponible y costes de aplicación, será preciso realizar una consulta previa a la Agencia Española de Protección de Datos tal y como establece el artículo 36 del RGPD.

a. Requisitos previos

Antes de realizar la consulta previa será necesario que se cumplan estos tres requisitos:

- Que el Ayuntamiento sea la responsable del tratamiento.
- Haber completado la EIPD del tratamiento afectado.
- Que la EIPD muestre un riesgo alto para los derechos y libertades de las personas tras haber aplicado medidas para mitigarlo.

b. Realización de la consulta

La consulta previa será llevada a cabo por el Ayuntamiento con el asesoramiento de la persona designada como delegado/a de Protección de Datos a través de la Sede Electrónica de la Agencia Española de Protección de Datos (sedeagpd.gob.es) a través del trámite Consulta previa al inicio de tratamientos de alto riesgo (art. 36 RGPD):

La consulta previa implicará la comunicación a la AEPD de la siguiente información:

- Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento.
- Los fines y medios del tratamiento previsto.
- Las medidas y garantías establecidas para proteger los derechos y libertades de las personas afectadas.
- Los datos de contacto del Delegado de Protección de Datos.
- La EIPD realizada.
- Cualquier otra información que solicite la Autoridad de Control.

En el informe EIPD se dejará constancia de la consulta previa remitida a la AEPD, así como un extracto de la información remitida.

c. Plazos de respuesta de la AEPD

La AEPD dispone de un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al Ayuntamiento y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58 del RGPD. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La AEPD deberá informar al Ayuntamiento de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la AEPD haya obtenido la información solicitada a los fines de la consulta.

d. Remisión de la información solicitada

La AEPD podrá solicitar aclaraciones o solicitar más información cuando sea preciso para analizar la consulta.

El Ayuntamiento deberá atender las peticiones de la AEPD sin dilación indebida y siempre dentro de los plazos previstos por la AEPD. La atención de las peticiones será supervisada por el Delegado de Protección de Datos.

e. Resolución de la AEPD

La AEPD podrá establecer la adopción de medidas para que el tratamiento de los datos pueda llevarse a cabo o por el contrario indicar la imposibilidad de realizar el tratamiento si el mismo supone un grave riesgo para las libertades y derechos de las personas afectadas.

El Ayuntamiento sólo llevará a cabo el tratamiento cuando la AEPD haya indicado que el tratamiento puede llevarse a cabo aplicando las medidas y siempre y cuando el Ayuntamiento pueda aplicar las mismas. En el caso de que la AEPD haya indicado que el tratamiento no puede llevarse a cabo o que el Ayuntamiento no puede aplicar las medidas de seguridad indicadas, no se realizará el tratamiento, dejando constancia en el informe EIPD de la decisión adoptada.

11 Fases de la EIPD. Revisión.

Como última fase del modelo de mejora continua en la realización de una EIPD, se precisa llevar a cabo una revisión periódica de posibles cambios en las actividades u operaciones de tratamiento, así como el estudio y análisis de las nuevas amenazas que se pudieran materializar y un seguimiento de la efectividad y eficacia de los controles y medidas de seguridad implementados. En caso de producirse cambios sustanciales en alguno de los parámetros descritos, se deberá realizar de nuevo una EIPD generando un nuevo informe y plan de acción que minimice los riesgos para los derechos y libertades de las personas interesadas en relación con el tratamiento de sus datos personales.

En caso de que los cambios sobre el tratamiento no sean significativos, y no generen por tanto nuevas amenazas y riesgos sobre los derechos y libertades de las personas afectadas, igualmente se debe realizar una valoración de los cambios producidos y documentar claramente la no necesidad de implantar nuevas medidas de control adicionales.

12 Actualización del documento

La actualización del presente documento corresponde a la persona designada como delegado/a de Protección de Datos del Ayuntamiento.