zegarra & schipper
abogados consultores

**LA AEPD PUBLICA UNA LISTA DE VERIFICACIÓN PARA AYUDAR A LOS RESPONSABLES DEL TRATAMIENTO DE DATOS PERSONALES A REALIZAR EVALUACIONES DE IMPACTO EN PROTECCIÓN DE DATOS**

En fecha 17 de febrero de 2022, la Agencia Española de Protección de Datos (AEPD) publicó un documento que contiene una lista de verificación para ayudar a los responsables del tratamiento de datos personales a identificar y determinar, de forma célere, el proceso e información que se procesa al realizar una Evaluación de Impacto relativa a Protección de Datos Personales (en adelante, Lista de Verificación")[1].

**1. ¿Qué es la Evaluación de Impacto referente a la Protección de Datos?**

La Evaluación de Impacto referente a la Protección de Datos (EIPD) es definida como un proceso para describir el tratamiento, evaluar su necesidad y proporcionalidad; así como para ayudar a gestionar los riesgos para los derechos y libertades de los titulares de los datos personales derivados del tratamiento de los datos personales, de modo que se evalúan los riesgos y se determinan las medidas para abordarlos.

**2. ¿En que consiste la Lista de Verificación?**

La Lista de Verificación tiene como objetivo entonces identificar y determinar si la Evaluación de Impacto en Protección de Datos cuenta con todos elementos formales mínimos que se espera de este.

La utilidad de la Lista de Verificación reside en ser una herramienta para comprobar, y en su caso declarar, que se han realizado las mínimas acciones formales requeridas para llevar a cabo una EIPD. La guía para la Gestión de riesgo y evaluación de impacto en tratamientos de datos personales aprobada por la AEPD desarrolla los detalles de las tareas y los contenidos mínimos que deberán ser tenidos en cuenta en la ejecución y documentación de la EIPD.

Así, se señala que no dar respuesta a dichos contenidos puede suponer que la EIPD es incompleta o que la información proporcionada es inexacta.

**3. ¿Cuál es el contenido de la Lista de Verificación?**

La Lista de Verificación desarrolla el contenido formal que debe incluir la documentación de la EIPD con el objeto de determinar dicha adecuación, en particular, para su presentación en el marco de una consulta previa[2], en los siguientes términos:

- Requisitos generales para la consulta previa: se debe considerar los requisitos y detallar la información adicional referida a nivel de riesgo del tratamiento; y, el carácter previo o posterior a la puesta en marcha del tratamiento.
- Requisitos del Delegado de Protección de Datos Personales

[1] Véase en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-lista-verificacion-para-ayudar-responsables-evaluaciones

[2] La AEPD señala que el proceso de consulta previa tiene como objeto presentar ante la Autoridad de Control un tratamiento que sea conforme con el Reglamento General de Protección de Datos, que tenga obligación o se haya valorado la oportunidad, o conveniencia, de realizar una EIPD, pero que entrañe un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptable, conforme a la guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

zegarra & schipper
abogados consultores

(DPD): se debe comprobar si el DPD ha sido nombrado o comunicado a la Autoridad de Control; si el responsable ha recabado su asesoramiento que se le ha solicitado; y, si el DPD supervisa la aplicación de la EIPD.

- Identificación del tratamiento de los datos personales e intervinientes y/o responsables.
- Actualización de una consulta previa: se debe señalar las modificaciones, el contexto, el ámbito, los fines, los riesgos y las garantías en el tratamiento; así como una referencia expresa a la respuesta o respuestas de la Autoridad o Autoridades de Control.
- Contexto del tratamiento y la EIPD: se describen los contextos internos y externos en los que se desenvuelve el tratamiento; y, las políticas de protección de datos personales aplicables.
- El tratamiento de datos personales debe cumplir con los requisitos de la normativa.
- Descripción sistemática del tratamiento: se requiere que se describa la naturaleza, el ámbito y el contexto del tratamiento; los casos de uso del tratamiento; se incluya un análisis estructurado del tratamiento; una descripción del ciclo de vida de los datos; la descripción de los activos, vulnerabilidades y amenazas implicados en el tratamiento; se identifiquen, implementen y/o documenten las medidas de privacidad; se detalle las cesiones de datos; se describa la certificación, sellos y marcas de protección de datos; y, √se identifiquen los códigos de conducta del tratamientos de datos.
- Análisis de obligación y análisis de necesidad de llevar a cabo el EIPD.
- Descripción del proceso de gestión formal de los riesgos para los derechos y libertades de los interesados.
- Análisis de la opinión de los interesados o de sus representantes en relación con el tratamiento previsto.
- Evaluación objetiva y positiva de la idoneidad, necesidad y la proporcionalidad del tratamiento de datos personales.
- Reevaluación de la EIPD y la caducidad del tratamiento: en el plan de acción de la gestión de riesgos para los derechos y libertades, se debe reflejar las acciones para la revisión y actualización de las medidas determinadas en la EIPD; la reevaluación periódica de la necesidad del tratamiento y la limitación de los datos utilizados; y, la inclusión de cláusulas de caducidad en las políticas de protección de datos.
- Acceso a la Autoridad de Control a toda la documentación que garantice que la información aportada es completa y exacta.

**4. Comentario**

La Lista de Verificación publicada por la AEPD es un documento de suma importancia para los responsables del tratamiento de datos personales, ya que ayuda a que estos realicen el EIPD, de manera célere y eficiente, identifiquen y gestionen los riesgos que se puedan presentar en el tratamiento de los datos personales respecto de los derechos y libertades de los titulares de los mismos.

zegarra & schipper
abogados consultores

De este forma es la propia autoridad administrativa la que desarrolla una labor de prevención de manera que con ello se logre un efectivo cumplimiento de la normativa sobre protección de datos personales y los responsables del tratamiento evite incurrir en infracciones administrativas.