LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES APRUEBA LA "GUÍA DE GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO EN TRATAMIENTO DE DATOS PERSONALES"

Con el objetivo de incorporar las lecciones aprendidas en la aplicación de la gestión del riesgo en el ámbito de la protección de datos personales, en fecha 29 de junio de 2021, la Agencia Española de Protección de Datos Personales (en adelante, la "AEPDP") ha publicado una "Guía de Gestión del Riesgo y Evaluación de Impacto en Tratamiento de Datos Personales" (en adelante, la "Guía"), en la que recopila los nuevos criterios e interpretaciones de la AEPDP, el Comité Europeo de Protección de Datos Personales (en adelante, el "CEPDP") y el Supervisor Europeo de Protección de Datos Personales (en adelante, el "SEPD").

A continuación, se desarrollará una reseña de los principales aspectos de dicho documento.

1. FUNDAMENTOS DE LA GESTIÓN DE RIESGOS PARA LOS DERECHOS Y LIBERTADES

La gestión del riesgo es un pilar de dirección de cualquier organización, y está formada por un conjunto de acciones orientadas a controlar las posibles consecuencias de una actividad sobre un conjunto de bienes que han de ser protegidos.

El Reglamento General de Protección de Datos Personales - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (en adelante, el "RGPD")[1], establece la obligación para los responsables y encargados del tratamiento de gestionar el riesgo que suponen sus actividades respecto a los datos personales, de salvaguardar posibles daños físicos, materiales o inmateriales, problemas de discriminación, usurpación de identidad, daño para la reputación o pérdida de confidencialidad de datos sujetos al secreto profesional.

Adicionalmente, en la Guía se señala que, la gestión del riesgo no solo debe tener un enfoque reactivo ante perjuicios hacia interesados, sino también preventivo denominado gestión proactiva del riesgo.

El proceso de gestión de riesgos señalado en la Guía cuenta con las siguientes etapas:

- **Descripción del tratamiento:** esta actividad implica un análisis profundo para llegar a conclusiones sobre la afectación de derechos y libertades.

- **Evaluación del nivel de riesgo y determinación de si procede o es necesario realizar una Evaluación de Impacto en Protección de Datos (en adelante, la "EIPD"):** se trata de una disciplina consolidada que requiere de la realización de tres actividades; i) identificar los factores de riesgo o amenazas para los derechos y libertades; ii) analizar los cada uno de ellos en su impacto y probabilidad; y, iii) evaluar el nivel global del riesgo del tratamiento para los derechos y libertades del tratamiento.

- **Tratamiento del riesgo:** en esta etapa se ejecutan acciones para reducir, eliminar o asumir de forma controlada los riesgos identificados. Se reduce ya sea la posibilidad de que se materialice un perjuicio o el impacto que genera. Implica adoptar medidas y garantías jurídicas.

- **Seguimiento y verificación de la eficacia de las medidas adoptadas y decisión sobre realizar un**

[1] **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo - Reglamento General de Protección de Datos Personales:**
"Artículo 23.- Limitaciones
El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar (...):
g) Los riesgos para los derechos y libertades de los interesados".

proceso de revisión y reevaluación de las medidas: la organización debe implementar procedimientos que detecten cambios en el tratamiento que sean susceptibles de desencadenar la necesidad de iniciar un ciclo de revisión de la gestión del riesgo. En caso no se detecten, se deben establecer periodos de revisión.

El proceso de gestión de riesgos se debe integrar a las políticas de protección de datos personales que debe realizarse bajo la idea de gobernanza de riesgos, conforme se dispone en el artículo 24[2] del RGPD.

2. APLICACIÓN PRÁCTICA DE LA GESTIÓN DE RIESGOS PARA LOS DERECHOS Y LIBERTADES

En la Guía se precisa que el tratamiento de datos se estudia a través de tres herramientas: i) estudios a alto nivel; ii) análisis de la estructura; y, iii) análisis del ciclo de vida de los datos.

Así, mediante dichos estudios se consigue la información suficiente sobre el contexto, naturaleza, ámbito y fines, así como el ciclo de uso de los datos para estudiar las etapas desde su recolección hasta su destrucción.

En cuanto a la identificación de los factores de riesgo, en la Guía se señala que deben analizarse según su nivel de impacto (significativo/limitado) y su nivel de probabilidad de ocurrencia (alta/baja).

Para que el riesgo identificado se reduzca a niveles aceptables, se adoptan medidas y garantías que apunten a determinadas finalidades: i) minimizar recopilaciones de datos que no son necesarios para las finalidades concebidas; ii) ocultar información confidencial; iii) separar, evitar que distintos datos se procesen en una misma entidad; iv) abstraer, evitar al máximo el detalle sobre los datos; v) informar sobre el tratamiento; vi) proporcionar control a los administrados; vii) cumplir con las políticas respectivas; y, viii) demostrar el cumplimiento de las políticas.

Por último, se debe evaluar siempre el riesgo residual que se obtiene luego de aplicadas las medidas, con las cuales se determina que no se obstruya la viabilidad del tratamiento.

3. EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS PERSONALES

La EIPD forma parte indivisible de la gestión de riesgos para derechos y libertades, que es un proceso de obligatorio cumplimiento para los responsables y encargados del tratamiento que debe ser realizado incluso antes de llevar a cabo la ejecución del tratamiento, según lo establecido en el artículo 35[3] del RGPD.

Acorde con lo señalado en la Guía, la realización de EIPD no será necesaria en caso de que se haya realizado una EIPD previa o cuando aparezca una lista orientativa de la Autoridad de Control que indique que no requiere ser ejecutada.

Debe tomarse en cuenta, según lo previsto en el artículo 35.7[4] del RGPD, que el EIPD siempre implica un análisis de necesidad y proporcionalidad del tratamiento, en la que se evalúe la: i) idoneidad; ii) necesidad; y, iii) proporcionalidad.

---

[2] **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo - Reglamento General de Protección de Datos Personales:**
*"**Artículo 24.- Responsabilidades del responsable del tratamiento** (...)*
Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos".

[3] **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo - Reglamento General de Protección de Datos Personales:**
*"**Artículo 35.- Evaluación de impacto relativa a la protección de datos** (...)*
1. El responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales".

[4] **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo - Reglamento General de Protección de Datos Personales:**
*"**Artículo 35.- Evaluación de impacto relativa a la protección de datos** (...)*
7. La evaluación deberá incluir como mínimo: (...)
b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad".

En el juicio de idoneidad, se debe evaluar si la propuesta de tratamiento, tal y como está planteada, alcanza la eficacia necesaria para cumplir los fines que persigue.

En el juicio de necesidad, se evalúa si, para la finalidad perseguida existe un tratamiento alternativo que sea igualmente eficaz para el logro de dicha finalidad.

En el juicio de proporcionalidad, se indica si los beneficios del tratamiento exceden o no a las limitaciones o intromisiones en la privacidad o en otros derechos de los interesados.

Según lo señalado en la Guía, tanto el responsable del tratamiento como el encargado pueden formular consultas ante la Autoridad de Control, con la finalidad de poder realizar adecuadamente el EIPD.

4. COMENTARIO

La publicación de la "Guía de Gestión del Riesgo y Evaluación de Impacto en Tratamiento de Datos Personales" de la AEPDP, constituye un documento de gran utilidad para los responsables del tratamiento puesto que permite enfocar la gestión de riesgos y las evaluaciones de impacto como medios eficaces de salvaguarda de derechos y libertades de los interesados.

En tal sentido, las pautas de la guía permiten mejorar la reputación empresarial como consecuencia de una gestión proactiva de riesgos, por lo que, es recomendable su consideración en el ordenamiento jurídico peruano a fin de que se optimicen las prácticas respecto al tratamiento de datos personales, fundamentalmente a partir de la aplicación del análisis de necesidad y proporcionalidad.