La Agencia Española de Protección de Datos Publicó una nueva versión de su Guía para notificar brechas de datos personales

En el año 2018, con la entrada en vigencia del Reglamento General de Protección de Datos del Parlamento Europeo y del Consejo de la Unión Europea (en adelante, RGPD), la Agencia Española de Protección de Datos (en adelante, AEPD) emitió una guía cuyo fin era ayudar a los responsables en el cumplimiento de sus obligaciones en lo referente a las brechas de datos personales. En mayo del 2021, la AEPD publicó una actualización de tal instrumento.

Dicha actualización añade ciertos contenidos normativos en base a la experiencia obtenida desde el 2018, sumando medidas como la creación de un entorno más resiliente basado en el conocimiento de las vulnerabilidades de las organizaciones (públicas o privadas) y la disposición de un medio para los responsables del tratamiento de datos personales a fin de que puedan demostrar diligencia en el cumplimiento de sus obligaciones.

Asimismo, desarrolla los conceptos básicos a tener en cuenta en la notificación de brechas de datos personales.

Los principales aspectos incorporados en la guía en su versión actualizada son:

1. **Brechas de Datos Personales**

En el marco de lo dispuesto en el artículo 33 del RGPD, la guía define a las brechas personales como "todas aquellas violaciones de la seguridad que ocasionen 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".

Adicionalmente, la guía hace especial énfasis en la exclusión de esta calificación cuando los incidentes no afecten datos personales, es decir, datos de personas naturales; cuando no afecten a trtamientos de datos por parte de un responsable o encargado; y cuando estos tratamientos se den en un contexto doméstico.

2. **Proceso de Gestión de Incidentes**

La guía establece algunas medidas para prevenir y procesar las brechas de datos personales. En primer lugar, como medidas preventivas de seguridad, plantean identificar el nivel de los riesgos existentes; luego, establecer garantías de confidencialidad, integridad y disponibilidad, así como garantizar la resiliencia de los sistemas, la seudonimización y el cifrado de datos.

Adicionalmente, se señala la obligación del responsable de ser diligente en la detección y calificación de un incidente como Brecha de Datos Personales, razón por la que se recomienda incorporar un procedimiento de notificación que defina cuál es la Autoridad de Control a la que se debe notificar, qué sucesos activan el procedimiento, quién debe notificar a la Autoridad de Control y el aseguramiento en el cumplimiento de plazos.

De la misma manera, la guía ofrece una herramienta denominada "Facilita-Emprende", mediante la cual, a través de la web, es posible obtener un modelo de registro de incidentes para empresas dentro del ámbito de aplicación del Reglamento.

3. **Comunicación a los titulares de los datos personales**

La guía establece que al ser los titulares de los datos personas naturales cuyos datos personales han sido comprometidos, se les deberá comunicar sobre el incidente, debiendo establecerse un procedimiento de comunicación en caso de una Brecha de Datos Personales.

En ese sentido, la guía ofrece una herramienta denominada "Comunica-Brecha RGPD" que ofrece ayuda a través de la web a los responsables del tratamiento de datos personales a fin de facilitar la comunicación de la Brecha a los afectados.

La guía determina que no será obligatorio que el responsable comunique al afectado en los supuestos en los que ha tomado medidas adecuadas que eviten los riesgos previos a la Brecha, revirtiéndose el daño a los derechos y libertades; y cuando el responsable ha tomado medidas de protección que mitigan total o parcialmente el posible impacto para los afectados, garantizando que no haya posibilidad de que el riesgo de daño a los derechos y libertades se materialice.

Asimismo, se aclara que el RGPD no establece un plazo para la comunicación con los afectados, pero la guía sí establece que deberá efectuarse sin dilación indebida en tanto se analice y concluya que se ha producido una Brecha afectando la integridad, confidencialidad o seguridad de los datos proporcionados.

De ese modo, la guía establece que la comunicación con el titular de los datos pesonales deberá describir la naturaleza de la violación de la seguridad de datos personales en un lenguaje claro y sencillo que contenga como mínimo:

a) Los datos de contacto del Delegado de Protección de Datos,
b) La descripción general y momento del incidente, y
c) Las consecuencias del incidente con las medidas implantadas para controlar los posibles daños.

4. Contenido y Plazo de las notificaciones de Brechas de Datos Personales a la Autoridad de Control

Dentro de los alcances normativos del RGPD, la guía desarrolla el contenido de las notificaciones a la Autoridad de Control, las cuales deberán estar compuestas por la información general sobre el tratamiento, la intencionalidad y el origen de la Brecha, la tipología, las categorías de datos y el perfil de los titulares de los datos personales, las consecuencias potenciales de la Brecha, las implicaciones tansfonterizas, los medios de detección de la Brecha, las medidas de seguridad antes del incidente, las acciones tomadas en base al incidente, la comunicación a los afectados y la identificación de los intervinientes.

Además, se establece que el plazo de notificación a la autoridad no deberá ser mayor a 72 horas luego del conocimiento de la Brecha.

5. Régimen Sancionador relativo a las Obligaciones del Artículo 33 y 34 del Reglamento

De acuerdo con los artículos 33 y 34 del Reglamento, el responsable del tratamiento de datos personales deberá notificar a la Autoridad de Control y comunicar del suceso a la víctima afectada en caso ocurra una vulneración a la seguridad de los datos personales.

No obstante, la guía esclarece que estas medidas evidenciarán la diligencia de la organización al momento de ejecutar la obligación de responsabilidad proactiva en el tratamiento de datos si se llevan a

cabo de forma oportuna, por lo que no necesariamente la notificación y la comunicación de la vulneración implicarían la imposición de una sanción.

En ese sentido, la guía sostiene que la ausencia de notificación a la Autoridad y la comunicación oportuna a la persona afectada por la Brecha de Datos Personales sí implicaría una sanción, de acuerdo con el artículo 58 del RGPD, el cual ha otorgado poderes correctivos a las Autoridades de Control a fin de que puedan ordenar al responsable del tratamiento que comunique al interesado la Brecha, y que imponga multas administrativas.

6. La Guía para notificar brechas de datos personales y la legislación peruana

Es importante anotar que no existe en el ordenamiento peruano una obligación del titular del banco de datos de notificar a la Autoridad de Protección de Datos Personales (En adelante, "APDP") en caso suceda una brecha de datos personales.

No obstante, en la Directiva de Seguridad emitida por la APDP, sí se estipula un deber de registrar los incidentes de seguridad relacionados con los bancos de datos. Este registro deberá contener como mínimo la fecha y hora del incidente, el nombre de la persona que lo reporta, la naturaleza del incidente, los datos comprometidos, consecuencias del incidente y las recomendaciones para el titular del banco de datos.

En ese sentido, si bien este ámbito está regulado, sería útil que la obligación de notificar a la Autoridad sobre los incidentes sea también contemplada en Perú. La razón de ello es que la coordinación con la entidad frente a estos eventos podría ofrecer un enfoque regulatorio más colaborativo y esta experiencia podría desarrollar mejores medidas de diligencia frente a un incidente de brecha de datos personales.

Asimismo, un procedimiento de gestión de riesgos posterior al incidente sería también un aporte destacable a la regulación peruana. Más aún si se encuentra sistematizado y delimitado como en la Guía de la Agencia Española, lo cual protegería mejor los datos y generaría mayor seguridad jurídica para los titulares de los bancos de datos frente a la imposición de sanciones.