LA OEA PUBLICÓ LOS PRINCIPIOS ACTUALIZADOS SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

El Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos (en adelante, "OEA") publicó el pasado 28 de enero de 2022, los Principios Actualizados sobre la Privacidad y Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021.

Se han publicado 13 Principios Actualizados que reflejan las aproximaciones predominantes en los Estados miembros sobre los temas centrales de la protección de datos personales. Además, en la publicación se incluyen las anotaciones que detallan los conceptos que constituyen el contenido de cada uno de los Principios Actualizados.

El ámbito de aplicación de los Principios Actualizados incluye tanto a los datos personales generados, recopilados o administrados por entidades públicas como privadas.

A continuación, se realiza una breve reseña de los Principios Actualizados:

1. **Finalidades Legítimas y Lealtad**

Los datos personales deben ser recopilados únicamente para finalidades legítimas y a través de medios leales y legítimos.

2. **Transparencia y Consentimiento**

Previamente y/o durante la recopilación de los datos personales, se debe informar a los titulares de los mismos sobre lo siguiente: (i) la identidad y los datos de contacto del responsable del tratamiento, (ii) las finalidades específicas para las cuales se tratarán los datos personales, (iii) la base legal que legitima su tratamiento, (iv) los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida; y, (v) los derechos del titular en relación al tratamiento de sus datos personales.

Cuando el tratamiento se base en el consentimiento, los datos personales deben ser recopilados con el consentimiento previo, inequívoco, libre e informado del titular de los mismos.

3. **Pertinencia y Necesidad**

Se debe garantizar que los datos personales sean adecuados, pertinentes, y se recopilen los mínimos necesarios en función a las finalidades específicas de su recopilación y posterior tratamiento.

4. **Tratamiento y Conservación Limitados**

Los datos personales deberían ser tratados y conservados solamente de manera legítima compatible con las finalidades para las cuales se recopilaron. Además, estos deberán ser conservados el tiempo necesario para cumplir dichas finalidades, teniendo en consideración la legislación nacional correspondiente.

5. **Confidencialidad**

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, salvo se cuente con el consentimiento del titular de los datos personales o bajo autoridad de la ley.

6. **Seguridad de los Datos**

La confidencialidad, integridad y disponibilidad de los datos personales debe garantizarse a través de medidas de seguridad técnicas, administrativas u organizacionales

razonables y adecuadas para contrarrestar los tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando éstos sean accidentales. Es importante que las medidas de seguridad sean objeto de auditoría y actualización permanente.

7. Exactitud de los Datos

Los datos personales deben mantenerse exactos, completos y actualizados tomando como límite objetivo la finalidad del tratamiento.

8. Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Es necesario que los responsables del tratamiento de los datos personales cuenten con métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como ejercer su derecho de oposición y, en lo aplicable, el derecho a la portabilidad de esos datos personales.

El ejercicio de los derechos mencionados debe ser gratuito. En caso se necesite restringir los alcances de estos derechos, se debe señalar expresamente las bases de cualquier restricción en la legislación nacional y estar en concordancia con lo dispuesto en los estándares internacionales aplicables.

9. Datos Personales Sensibles

La sensibilidad de algunos datos personales en contextos específicos puede causar daños considerables a las personas si se hace mal uso de ellos. Por ello, las categorías de estos datos y el alcance de su protección se deben indicar claramente en la legislación y normativas nacionales.

10. Responsabilidad

Los responsables y encargados del tratamiento de datos deben implementar medidas técnicas y organizacionales que sean apropiadas para garantizar el cumplimiento de estos principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente.

El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

11. Flujo Transfronterizo de Datos y Responsabilidad

Los Estados Miembros deben cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, dicha cooperación también debe incluir la creación de mecanismos destinados a asegurar que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o transmitan los datos a una jurisdicción distinta de la suya, puedan garantizar y ser responsables por el cumplimiento de estos Principios.

12. Excepciones

Las excepciones a estos Principios deberán estar previstas de forma expresa y específica en los ordenamientos jurídicos nacionales, la cual debe ser puesta en conocimiento del público y limitarse a únicamente los siguientes motivos: (i) soberanía nacional, (ii) seguridad nacional, (iii) seguridad pública, (iv) protección de la salud pública, (v) el combate a la criminalidad, (vi) el cumplimiento de normativas u otras prerrogativas de orden público; y, (vii) el interés público.

13. Autoridades de Protección de Datos

Es necesario la implementación de órganos de supervisión independientes por parte de los Estados Miembros, de acuerdo con la estructura constitucional, organizacional y administrativa de cada Estado, con el objetivo de supervisar y promover la protección de datos personales de acuerdo con estos Principios. Asimismo, los Estados Miembros deben promover la cooperación entre tales órganos.

Comentario:

La publicación de la OEA responde a la necesidad de detallar los principios sobre la protección de datos personales teniendo en cuenta la evolución de los mismos y su desarrollo en los Estados Miembros, puesto que dichos principios habían sido adoptados originalmente por el CJI en el 2012.

Los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, se configuran como un instrumento de *soft law* interamericano que tiene como finalidad servir de referencia a los Estados Miembros de manera que puedan fortalecer sus ordenamientos jurídicos en relación al derecho de protección de datos y se fomente la cooperación entre los mismos como un mecanismo para garantizar el cumplimiento de los principios.