Protección de Datos Personales – Sesión 2

Msc. Christian Hidalgo García

Qué es el GDPR

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) es la nueva normativa europea de privacidad.

Es una ley que entro en vigor en el 2018 y establece las normas sobre cómo las empresas y organizaciones deben recopilar, usar, almacenar y proteger datos personales de las personas que residen en la UE

Objetivos principales del GDPR

- **Proteger la privacidad de los ciudadanos de la UE**
- **Unificar las leyes de protección de datos de los países miembros**
- **Dar más control a los individuos**

¿Qué regula?

- Qué datos se pueden recolectar
- Cómo deben obtenerse los consentimientos
- Cómo deben almacenarse y protegerse los datos
- Qué derechos tienen los usuarios sobre sus datos
- Qué hacer en caso de violaciones de seguridad

Los principios básicos que rigen el GDPR

- 1. Transparencia. Las organizaciones deben informar a los ciudadanos sobre la licitud de la captación y uso de sus datos personales.
- 2. Consentimiento claro y expreso. Las empresas sólo pueden utilizar los datos para los fines específicos para los que fueron recopilados.
- 3. Minimizar la recopilación. La captación de datos indiscriminada no estará permitida. Las organizaciones podrán recoger sólo aquellos datos pertinentes para el fin previsto.
- 4. Exactitud de la información, derecho al olvido y portabilidad. Los ciudadanos podrán exigir la modificación, borrado o traspaso a terceros de sus datos personales contenidos en los ficheros de las compañías.
- 5. Almacenamiento limitado. Los datos personales sólo podrán ser almacenados por el tiempo necesario para lograr los fines para los que fueron recogidos.
- 6. Garantía de seguridad. Las organizaciones deben garantizar la seguridad y confidencialidad de los datos personales almacenados.

1. El principio de Licitud, lealtad y Transparencia

- Los datos deben tratarse de manera legal, justa y transparente para el interesado

- La persona debe saber qué datos se recogen, para qué y cómo se usarán.

2. Limitación de la finalidad (propósito)

Los datos deben recogerse **con fines específicos, explícitos y legítimos**, y **no deben usarse para otros fines** distintos sin consentimiento adicional.

3. Minimización de los datos

Los datos personales que deben recopilarse deben ser “adecuados, relevantes y limitados a lo que sea necesario en relación con los fines para los que se procesan”

4. Exactitud

Los datos deben ser **precisos y estar actualizados**. Si son incorrectos, deben corregirse o eliminarse lo antes posible.

5. Limitación del plazo de conservación

Los datos personales deben “mantenerse en una forma que permita la identificación de los interesados por un periodo no superior al necesario”. Se debe establecer cuál es el período de retención para los datos personales que recopilas y justificar que este período es necesario para los objetivos específicos.

6. Integridad y confidencialidad

Se deben aplicar medidas técnicas y organizativas adecuadas para **garantizar la seguridad**, confidencialidad e integridad de los datos.

7. El principio de responsabilidad proactiva

Hace referencia a la obligación de las organizaciones de garantizar técnicamente el cumplimiento del GDPR. Engloba varias medidas que toda entidad debe tener en cuenta y que sirven como hoja de ruta para el diseño de un proceso estándar de tratamiento de datos

- Protección de datos desde el diseño
- Protección de datos por defecto
- Medidas de seguridad
- Mantenimiento de un registro de tratamientos
- Realización de evaluaciones de impacto sobre la protección de datos
- Nombramiento de un delegado de protección de datos
- Notificación de violaciones de la seguridad de los datos
- Promoción de códigos de conducta y esquemas de certificación

Medidas de responsabilidad activa

- Análisis de riesgo
- Registro de actividades de tratamiento e Inventario.
- Protección de Datos desde el Diseño y por Defecto
- Medidas de seguridad
- Notificación de "violaciones de seguridad de los datos"
- Evaluación de Impacto sobre la Protección de Datos
- Oficial de Protección de Datos

Protección de datos desde el diseño

La **protección de datos desde el diseño** (es un concepto clave del GDPR y está regulado específicamente en el **Artículo 25**. Este principio exige que la protección de datos personales se tenga en cuenta **desde el inicio mismo** del desarrollo de productos, servicios o procesos que impliquen el tratamiento de datos personales.

- **Integrar medidas de privacidad desde la fase de diseño** de sistemas, aplicaciones o servicios.
- **Prever los riesgos para la privacidad** antes de que ocurran y minimizarlos desde el principio.
- Aplicar **medidas técnicas y organizativas** adecuadas que garanticen que solo se procesen los datos personales

Protección de datos por defecto

- El principio de protección de datos por defecto supone la puesta en práctica del principio de minimización de datos mediante las medidas técnicas y organizativas que garanticen, por defecto, que únicamente sean objeto de tratamiento los datos necesarios para los fines del mismo y que hubieran sido definidos en la etapa de diseño inicial.

Registro de actividades de tratamiento

- ❑ el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- ❑ los fines del tratamiento.
- ❑ una descripción de las categorías de interesados y de las categorías de datos personales
- ❑ las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- ❑ en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo2, la documentación de garantías adecuadas;
- ❑ cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- ❑ cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Designación de un delegado responsable de datos

Todas las organizaciones deberán nombrar un representante que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos. Los datos de contacto de ese representante deberán proporcionarse a los interesados.

Notificación de violación de seguridad de los datos

Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Evaluación de Impacto sobre Protección de Datos

La **Evaluación de Impacto sobre la Protección de Datos** (EIPD o *DPIA*, por sus siglas en inglés: *Data Protection Impact Assessment*) es un proceso obligatorio en ciertas situaciones bajo el **GDPR**, regulado en el **Artículo 35**.

Es un **análisis sistemático** que permite identificar, evaluar y minimizar los riesgos que un tratamiento de datos personales podría tener para los derechos y libertades de las personas.

Promoción de códigos de conducta y esquemas de certificación

Los códigos de conducta constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas.

En materia de protección de datos, son mecanismos de cumplimiento voluntario en los que se establecen reglas específicas para categorías de responsables o encargados del tratamiento con la finalidad de contribuir a la correcta aplicación del Reglamento general de protección de datos (RGPD

El enfoque de riesgo

- Se refiere a que la aplicación de las medidas previstas por el GDPR deben adaptarse a las características de las organizaciones y el tipo de datos que tratan. No tendrá que cumplir con las mismas obligaciones una compañía que recaba datos de carácter sanitario, o volúmenes de datos de millones de interesados, que una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Protocolos mínimos

DOCUMENTOS

- Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable

CAPACITACION

- Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales

TRAZABILIDAD

- Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad

ATENCION

- Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento

HISTORIAL

- Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento.

TRANSFERENCIA

- Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos.

Gobernanza de Datos

“La gobernanza de los datos es un sistema de derechos de *decisión y responsabilidades* para los procesos relacionados con la información, ejecutados según modelos acordados que describen **quién** puede tomar **qué** acciones, **con qué** información, y **cuándo**, en **qué circunstancias**, utilizando **qué métodos”** (Definición del Data Governance Institute)

SULÁ BATSÚ COOPERATIVA

- Ley de Acceso a la Información Pública (LAIP)

- Ley para la Implementación de Datos Abiertos en Guatemala

Muchas Gracias

Christian Hidalgo García
www.sulabatsu.com
Christian@sulabatsu.com

SULÁ BATSÚ
COOPERATIVA