ateneu

PRIVACY CONSULTING

El nuevo Reglamento de Protección de Datos

Objetivo del GDPR: La cultura de privacidad

El nuevo Reglamento europeo (GDPR) pretende que todas las empresas y organizaciones que tratan datos de ciudadanos europeos, sean locales o internacionales, se atiendan a una única legislación en toda la UE, evitando así diferencias de criterios y regímenes sancionadores según el país en el que se realice el tratamiento.

Esta nueva normativa va a fortalecer nuestros derechos delante de la comunidad internacional y seguramente va a posibilitar el cambio de leyes en otros países en esta materia, para armonizar estos derechos individuales en todo el mundo.

Con el GDPR, la protección de los datos personales se convertirá en algo más que un cumplimiento formal de obligaciones legales como venía siendo hasta ahora. La nueva regulación pretende propiciar una verdadera cultura de la privacidad.

La figura del consultor de privacidad es de gran relevancia para alcanzar este objetivo, poniendo sus conocimientos a disposición del tejido empresarial del país para para razonar la normativa, asesorar en los procedimientos a implementar y resolver las incidencias que se puedan producir.

Periodo de transición: De la LOPD al GDPR

El GDPR entró en vigor en mayo de 2016 y será aplicable a partir del mayo de 2018. En este periodo transitorio, aunque sigue vigente la LOPD, los responsables y encargados de tratamiento deben ir adoptando las medidas necesarias para cumplir la nueva normativa en el momento de su aplicación.

El nuevo Reglamento es directamente aplicable y no requiere de normas internas de trasposición. Por ello, los responsables y encargados deben asumir que la norma de referencia es el GDPR y no la LOPD.

El RGPD contiene muchos conceptos similares a los establecidos en la LOPD, sin embargo contiene nuevas obligaciones que deben ser aplicadas por cada organización, especialmente el principio de responsabilidad proactiva (poder demostrar el cumplimiento) y el enfoque de riesgo (evaluaciones de impacto cuando exista un alto riesgo).

El GDPR es de obligado cumplimiento para cualquier persona física o jurídica, autoridad pública, servicio u organismo que, solo o por encargo, realice un tratamiento de datos personales de ciudadanos residentes en la UE, independientemente que el tratamiento se realice en la UE o no.

Novedades respecto a la LOPD

Legitimización del tratamiento

- Consentimiento explícito del interesado.
- Interés legítimo del responsable.
- Información clara y concisa del tratamiento basada en la transparencia.
- Información sobre el plazo de conservación de los datos y las transferencias internacionales.

Nuevos derechos del interesado

- Obtener una copia de los datos.
- Supresión de los datos (derecho al olvido).
- Limitación del tratamiento.
- Portabilidad de los datos.

Encargados de tratamiento

- Deberán certificar que ofrecen suficientes garantías para cumplir el GDPR.
- Prohibición de encargar un tratamiento sin un contrato o acto jurídico de protección de datos.

Responsabilidad proactiva

- Capacidad de demostrar el cumplimiento de todos los principios del tratamiento: Licitud, Limitación de los fines, Minimización de los datos, Exactitud, Limitación del plazo de conservación, Integridad y confidencialidad.

Medidas de seguridad

- Análisis de los riesgos del tratamiento.
- Protección de los datos desde el diseño y por defecto en cualquier fase del tratamiento.
- Garantizar un nivel adecuado de seguridad según las necesidades, tamaño, circunstancias, contexto y finalidades del tratamiento.
- Registro de las actividades de tratamiento.

Evaluaciones de impacto

- Nuevas tecnologías con un alto riesgo.
- Elaboración de perfiles con efectos jurídicos.
- Datos relativos a condenas y delitos penales.
- Tratamientos a gran escala de categorías especiales de datos u observación sistemática de una zona de acceso público.

Violaciones de datos

- Documentar las violaciones de seguridad.
- Notificarlas a la AEPD en un máximo de 72h.
- Comunicarlas directamente a los interesados.

Delegado de protección de datos

- Será obligatorio designar un DPO cuando:
- El tratamiento lo realice un Organismo público.
- La actividad principal del responsable contemple tratamientos a gran escala de:
    - Categorías especiales de datos.
    - Datos de condenas e infracciones penales.
    - Observación habitual y sistemática de interesados.

Sanciones

- Multas proporcionales a cada caso particular.
- Incremento de la cuantía sancionable que podrá llegar a 20.000.000 € o el 2% del total de la facturación anual del ejercicio financiero anterior.

Debemos prepararnos para el GDPR

En la medida que el GDPR nos propone una nueva cultura de privacidad, este es el momento para revisar nuestros procedimientos:

- Si no se está cumpliendo con la LOPD, deberemos ponernos al día, ya que la transición al GDPR será mucho más sencilla desde su cumplimiento.
- Regularizar las relaciones con los encargados de tratamiento, realizando un inventario de los mismos y redactar nuevos contratos que contemplen las obligaciones del GDPR.
- Implementar medidas de seguridad desde el diseño y por defecto en todos los procesos de tratamiento para permitir la protección de datos y el ejercicio de los derechos de los interesados.
- Realizar un análisis de los riesgos que atañen al tratamiento, asumiendo que la protección de datos es mucho más que un cumplimiento formal y documental.

ateneu.eu 977 441 939 Teodor Gonzàlez, 31. TORTOSA @ comercial@ateneu.eu