Tendencias de protección de datos en la industria aseguradora

El cumplimiento normativo que impacta en las entidades aseguradoras está en constante evolución y, en lo que respecta a la protección de datos, hay que destacar el nuevo Reglamento General de Protección de Datos (GDPR, en sus siglas en inglés). En este contexto, la industria aseguradora no puede quedar ajena al amplio espectro de novedades que incorpora el nuevo marco normativo, tal y como se puso de manifiesto en la Jornada Normativa en Distribución de Seguros: IDD - LDS - GDPR, celebrada en Afi Escuela de Finanzas.

Pablo Aumente @AumentePablo | *Consultor del área de Seguros de Afi*

«El 25 de mayo es el día que se enciende la llama olímpica». Con estas palabras comenzó su intervención como ponente D. José Luis Piñar Mañas[1], uno de los mayores expertos en protección de datos del panorama europeo *en la Jornada Normativa en Distribución de Seguros: IDD - LDS - GDPR, celebrada en Afi Escuela de Finanzas*[2]. En efecto, tan señalada fecha marca el comienzo de un **nuevo modelo de protección de datos basado en la responsabilidad proactiva** (artículo 24 GDPR). Es decir, los sujetos obligados han de diseñar, aplicar y demostrar que disponen de las medidas de seguridad, técnicas y organizativas oportunas (gobierno responsable) para garantizar que cumplen con la normativa. Este nuevo modelo supone un cambio de paradigma que afecta, entre otros, a ámbitos de especial sensibilidad para el sector asegurador.

¿Qué implicaciones tiene la desaparición del consentimiento tácito?

Entre las numerosas novedades que trae consigo el Reglamento, **el consentimiento tácito ya no será válido** para el tratamiento de los datos, y **se requerirá de un consentimiento expreso** para entender que aquél se ha otorgado. En esta línea, «*el silencio, las casillas pre-marcadas o la inacción no deben constituir consentimiento*» aclaró el profesor Piñar. De este modo, **los consentimientos tácitos obtenidos con anterioridad a la fecha de aplicación del GDPR no serán válidos**, ya que «*solo serán válidamente obtenidos si se obtuvieron conforme a lo establecido por el Reglamento*». Adicionalmente, en base al Principio del consentimiento, los datos no se podrán utilizar para una finalidad distinta para la que fueron recabados, y cuando ya no tengan utilidad se tendrán que cancelar (Principio de calidad del dato).

Entonces, ¿qué hacer con los datos recabados en pólizas de seguro que se dan de baja?

Si un cliente cancela una póliza, en principio no hay que borrar sus datos de manera inmediata. Se podrían mantener en la medida en que sean necesarios, por ejemplo, para la gestión de primas pendientes de cobro o tramitación de siniestros sujetos a resolución. Ahora bien, salvo supuestos como estos, **las compañías deberán eliminar todos los datos** en el momento que finalice la relación jurídica en su totalidad **salvo que se cuente con su consentimiento expreso**. Así, **en el caso de pretender volver a captar al tomador** que canceló la póliza con la compañía aprovechando los datos anteriores, habría que contar con su consentimiento expreso.

¿Se puede convertir un consentimiento tácito en explícito?

La posibilidad de conversión **se podría articular en base a conductas que puedan indicar que ha habido consentimiento explícito, pero ello conlleva analizar caso a caso** (por ejemplo, la comunicación efectuada por un cliente a la compañía aseguradora para que le envíen la revista corporativa a una nueva dirección).

También se puede invocar la figura del interés legítimo del Responsable de tratamiento de datos (como podría ser la mercadotecnia) para justificar la conversión de consentimientos tácitos en explícitos, pero tal y como dispone el propio Considerando 47 del GDPR, «***requeriría una evaluación meticulosa***, *inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin*».

¿Qué cautelas han de adoptarse con las categorías especiales de datos?

En el plano asegurador, además, tiene **especial incidencia la prohibición relativa al tratamiento de categorías especiales de datos**, entre los que se encuentran los **datos genéticos**, los **datos biométricos** que permitan la identificación unívoca de una persona o los **datos relativos a la salud**. En estos casos, además de las obligaciones impuestas para el tratamiento de estas categorías especiales de datos, se establece por defecto un **principio general de prohibición de tratamiento**. Sólo se exceptúan determinados supuestos como que el interesado haya dado su consentimiento explícito para fines específicos (excepto si está prohibido por la legislación vigente), que sea necesario para proteger los intereses vitales del interesado, o cuando el tratamiento esté fundamentado en la legislación vigente (entre otros supuestos).

Las aseguradoras diseñan una plantilla para el reporte de violaciones de datos sobre el nuevo GDPR, ¿cómo funciona?

En base al enfoque del riesgo, las empresas tienen que informar a la Agencia Española de Protección de Datos (AEPD) cuando hayan sufrido una brecha de seguridad. En este sentido, Insurance Europe ha desarrollado una **plantilla[3] para ayudar a las compañías de seguros** a cumplir con la obligación de **notificar las violaciones de datos personales**.

La plantilla está configurada de tal manera que **la información recogida pueda ser compartida sin necesidad de ser anonimizada o agregada**, ya que no será posible identificar a una empresa a través de la información que proporcione.

La plantilla tiene **3 secciones** distintas:

1. Datos personales e información sobre la empresa afectada (no compartida con terceros).

2. Detalles sobre el incidente de violación de datos (de conformidad con lo dispuesto en el Art. 33 GDPR), que se enviarán a la autoridad nacional de supervisión, cuando sea factible, a más tardar 72 horas después de haber tenido conocimiento de la violación.

3. Una sección que debe completarse una vez transcurrido el plazo de 72 horas en el que se dispone de más información sobre la violación de datos ::

---

[1] Catedrático de Derecho Administrativo; Delegado de Protección de Datos del Consejo General de la Abogacía Española; Ex-director de la Agencia Española de Protección de Datos (AEPD).

[2] Documentación de la Jornada disponible en: www.afi-research.es/InfoR/secciones/1601154/Talleres-y-jornadas.html

[3] https://www.insuranceeurope.eu/template-data-breach-notifications?&utm_source=exacttarget&utm_medium=email&utm_campaign=BDS+20+de+marzo+2018