20211010, Nota Informativa, sobre anonimización y aviso de seguridad.

En virtud de mis compromisos contractuales, seguidamente os participo del documento comentado en el Blog de la AEPD sobre las diferencias entre anonimización y seudonimización, y, también, el último aviso de seguridad emitido por la OSI (Oficina de Seguridad del Internauta, dependiente del INCIBE -Instituto Nacional de Ciberseguridad-) referente a que se han "identificado grupos en Telegram ofreciendo el certificado de vacuna COVID-19 o PCR negativa de forma ilegal".

Anonimización y seudonimización

La información anónima es un conjunto de datos que no guarda relación con una persona física identificada o identificable (Considerando 26 del RGPD), en tanto que la información seudonimizada es un conjunto de datos que no puede atribuirse a un interesado sin utilizar información adicional, requiere que dicha información adicional figure por separado y, además, esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable (Artículo 4.5).

Transformar un conjunto de datos personales en información anónima o seudonimizada exige realizar un tratamiento sobre dichos datos personales. El tratamiento de anonimización genera un único y nuevo conjunto de datos, mientras que el tratamiento de seudonimización genera dos nuevos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la anonimización.

El conjunto de datos anonimizados no está bajo el ámbito de aplicación del Reglamento General de Protección de Datos (RGPD) (Considerando 26) aunque pudiera estar bajo el ámbito de aplicación de otras normas (p. ej. de seguridad nacional, salud pública, infraestructuras críticas, etc.). En este caso debe tenerse en cuenta que:

- El tratamiento que generan los datos anonimizados sí es un tratamiento de datos personales, que puede considerarse compatible con el fin original del tratamiento de datos personales del que proceden los datos (Dictamen 05/2014 sobre técnicas de anonimización WP246 apartado 2.2.1. Legitimación del proceso de anonimización).
- El conjunto de datos anonimizados queda fuera del ámbito de aplicación del RGPD en la medida que es posible demostrar objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física determinada, directa o indirectamente, ya sea mediante el uso de otros conjuntos de datos, informaciones o medidas técnicas y materiales que pudieran existir a disposición de terceros.

Es decir, los datos se considerarán anonimizados en la medida que no exista una probabilidad razonable que cualquier persona pueda identificar a la persona física en el conjunto de datos. Dicha evaluación ha de tener en cuenta los costes, el tiempo requerido para llevar a cabo la reidentificación o los medios tecnológicos necesarios para conseguir la reversión de la anonimización, tanto los actuales como teniendo en cuenta los avances tecnológicos (Considerando 26).

El conjunto de datos seudonimizados, y la información adicional vinculada con dicho conjunto de datos, están bajo el ámbito de aplicación del RGPD, así como el tratamiento que los genera. De ahí que el conjunto de datos seudonimizados esté protegido por cuatro tipos de garantías: en primer lugar, el propio tratamiento de seudonimización que ha de impedir la reidentificación sin disponer de la información adicional; en segundo lugar, los principios y garantías del RGPD que establecen limitaciones, entre otras, a las finalidades, el periodo de conservación o la comunicación de los datos seudonimizados; en tercer lugar, las garantías adicionales que incorpore el tratamiento de los datos seudonimizados en función del riesgo para los derechos y libertades de las personas físicas; en cuarto lugar, derivado del anterior, las garantías técnicas y organizativas dispuestas al efecto de impedir la materialización de brechas de datos personales, tanto sobre conjunto seudonimizado como de la información adicional.

Por otro lado, sobre el conjunto de datos anonimizados, desde el punto de vista del RGPD, solo aplica un tipo de garantías: la robustez del proceso de anonimización contra la posible reidentificación. Una vez el conjunto de datos está anonimizado, desaparece la obligación de implementar los otros tres conjuntos de garantías, al menos desde el punto de vista de la normativa de protección de datos.

No obstante, seguirán siendo aplicables garantías que se pudieran derivar de otra normativa (ver apartado 2.2.3 del Dictamen 5/2014) y se podrían establecer limitaciones al tratamiento (por ejemplo, mediante condiciones incorporadas en licencias de uso de la información anonimizada).

Los derechos y libertades de los interesados han de estar igualmente protegidas tanto en los tratamientos de anonimización como en los

procesos de seudonimización. Teniendo en cuenta que sobre el conjunto de datos anonimizados no será preciso atender a los requisitos establecidos por el RGPD en cuanto a la limitación del tratamiento, la conservación de los datos, las comunicaciones y las transferencias internacionales, o las medidas para proteger la confidencialidad, se han de diseñar y validar los tratamientos de anonimización pensando en la protección de los derechos anteriormente señalados. Esto exige poder demostrar un nivel objetivo de calidad en el tratamiento de anonimización y aconseja determinar cómo evoluciona el riesgo de reidentificación a lo largo del tiempo.

Identificados grupos en Telegram ofreciendo el certificado de vacuna COVID-19 o PCR negativa de forma ilegal

Se han detectado varios grupos de Telegram en los que se ofrece ayuda para conseguir de forma ilegal el certificado de vacuna COVID-19 o PCR negativa. Los propios usuarios que han intentado obtener dicho certificado se han convertido en víctimas de un fraude tras haber realizado el pago para su obtención.

Recursos afectados

Cualquier usuario que haya intentado obtener un certificado de vacuna COVID-19 o PCR negativa de forma ilegal a través de Telegram u otras aplicaciones y haya realizado el pago.

Solución

Si has intentado obtener un certificado de vacuna COVID-19 o PCR negativa de forma ilegal y te has puesto en contacto con algún perfil que ofrece este servicio, pero no has facilitado datos personales, ni realizado ningún pago, únicamente elimina la conversación y bloquea

el contacto a través de Telegram o de la plataforma por la que hayas contactado.

Si has contactado con el perfil y has facilitado tus datos personales, únicamente te recomendamos realizar egosurfing (es decir, una búsqueda de tu nombre y otros datos personales en el buscador) de forma periódica. En el caso de encontrar que se está utilizando indebidamente información sobre ti, puedes ejercer tus derechos de acceso, rectificación, oposición y supresión al tratamiento de tus datos personales siguiendo las pautas que proporciona la Agencia Española de Protección de Datos.

En caso de haber realizado el pago solicitado por el ciberdelincuente, contacta lo antes posible con tu entidad bancaria para informarles de lo sucedido. Además, te recomendamos permanecer atento y monitorizar periódicamente tus movimientos bancarios.

Por último, si has sido víctima de este fraude, te recomendamos recoger todas las evidencias posibles (capturas de pantalla, e-mails, mensajes, etc.) y contactar con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) e INCIBE, a través de la Oficina de Seguridad del Internauta (OSI). Para ello, puedes hacer uso de algún testigo online.

En cualquier caso, quedo a vuestra disposición para aclarar cualquier duda referente a la presente Nota Informativa.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de octubre de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Digitally signed by ZOTANO SANCHEZ SALVADOR - 32028277H
Date: 2021.10.10 19:52:44 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)