Protección de datos apercibe a un abogado por tirar documentos de sus clientes a la basura

16-2-2021 | Wolters Kluwer

El pasado 21 de enero de 2021, la Agencia Española de Protección de Datos (AEPD) apercibe a un abogado por haber tirado dos bolsas de plástico repletas de documentación a la basura, en la que aparecen datos personales de distintos clientes, como escrituras, poderes notariales, sentencias, fotocopias de DNIs o testamentos. Según recoge el dictamen, fue la Sección del SEPRONA la que acudió a la AEPD en junio del año pasado después de encontrar toda la documentación junto a unos contenedores de basura.

Victoria Royo Pérez. No adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de los datos personales, así como no mantener los deberes de integridad y confidencialidad, puede llegar a constituir una "infracción grave" del RGPD, recogida en su artículo 32. En el caso expuesto, la AEPD indica que, las violaciones de seguridad de los datos personales pueden llegar a conllevar multas que, dependiendo de la gravedad de las conductas, pueden alcanzar 10 millones de euros como máximo o, para las empresas, el 2 % de su facturación anual a nivel global, optándose por la de mayor cuantía.

En este caso, no obstante, la AEPD rebaja la sanción al entender que aplicar lo dispuesto en el artículo 83.4.a RGPD constituiría "una carga desproporcionada para el reclamado". En su lugar, el organismo concluye que la existencia de un incidente de seguridad en los sistemas del abogado, que ha permitido que documentación con datos de carácter personal fuesen localizados junto a unos contenedores de basura, puede ser sancionado con un apercibimiento, de acuerdo con el artículo 58.2.b) del RGPD, puesto que, además, "no consta la comisión de ninguna infracción anterior en materia de protección de datos".

¿Cómo deben destruir sus documentos los abogados?

Esta reciente resolución de la AEPD, por lo tanto, apercibe a un abogado por tirar a la basura documentos con datos de sus clientes, advirtiendo por primera vez a los letrados de que este tipo de práctica de destrucción de documentos está prohibido. "Es importante que los abogados se conciencien del riesgo de desechar documentos sin su previa destrucción absoluta", apunta Tamara Vizcaíno, abogada experta en protección de datos en Grupo Adaptalia, "pero no solo por evitar el riesgo de sanción por parte de la AEPD, sino porque con estas prácticas podrían originar una brecha de seguridad, cuyas consecuencias más graves podrían ser, además de la sanción

económica y la pérdida de confidencialidad de los datos, el daño reputacional al que podría enfrentarse la organización".

En este sentido, los documentos que vayan a ser destruidos deben estar bloqueados y conservados hasta el momento de su destrucción física. Además, los contenedores donde se almacenen deben disponer de medidas eficaces frente a terceros. Vizcaíno sugiere no amontonar los contenedores con documentos en lugares de paso, ni en locales abiertos, "es aconsejable que dispongan de mecanismos de cierre que garanticen su seguridad".

En el caso por el que opte por la trituración del papel, la destrucción deberá hacer imposible la reconstrucción o recuperación de cualquier información contenida por los documentos. Una vez destruidos, no deben depositarse en contenedores al descubierto, ni en cajas abiertas, evitando siempre desecharlos en la vía pública al alcance de cualquier persona. Así, "las medidas de destrucción deben pasar siempre por una eliminación controlada y eficaz, incluso contando con empresas especializadas que certifican la destrucción y responden contractualmente", apunta Maitane Valdecantos, socia de Audens. "Pero nunca tirar expedientes, sin más, al contenedor", asevera la letrada.

Eso solo respecto a la destrucción de documentos en papel, pero en la actualidad, en un despacho la información se almacena en soportes digitales: pen drives, discos duros… En la Guía sobre almacenamiento y borrado seguro de información elaborada por INTECO (Instituto Nacional de Ciberseguridad), existen distintos métodos de destrucción de la información en medios digitales, como la desmagnetización, el borrado concreto con sobreescritura, o una destrucción total que los haga inservibles e irrecuperables, dependiendo del tipo de dispositivo que se pretenda eliminar. En este sentido, a la hora de elegir entre una u otra opción, según Vizcaíno lo más importante es que los activos se eliminen definitivamente del dispositivo, destruyendo toda la información contenida en ellos y, que a posteriori, se contrate una empresa externa que proceda a la eliminación física del soporte, emitiendo el correspondiente certificado de destrucción. No obstante, "todos esos elementos deberían estar cifrados de raíz, para evitar un acceso inoportuno en caso de que no se hubiera destruido adecuadamente un soporte", señala Valdecantos.

Medidas de seguridad en el tratamiento de datos en despachos

De conformidad con el RGPD, las medidas de seguridad se deberán incorporar teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Estas medidas técnicas dependerán mucho del tipo de datos tratados por el despacho. Para que éstos determinen dichas medidas, será fundamental realizar un análisis de los diferentes tratamientos que realizan a efectos de determinar concretamente las medidas adecuadas que se deberá aplicar a cada tratamiento

Así, los expertos en este campo apuntan que, además de las medidas técnicas, tiene gran importancia la formación y concienciación de las personas que gestionan o acceden a los documentos con datos personales, ya que ellos son el principal elemento de riesgo. "Una vez que se tiene una adecuada política de concienciación, se aplican medidas de seguridad específicas según el tipo de datos personales e información que contenga el documento", comenta Maitane Valdecantos.

En este sentido, de conformidad con el principio de minimización de datos impuesto por el artículo 5.1 c) RGPD, el tratamiento de datos deberá quedar limitado a satisfacer la finalidad para la cual fueron recabados. "En el momento en que finaliza la relación profesional estos deberán ser bloqueados, lo cual no significa la eliminación completa de todos los datos personales y de la documentación física", apunta Vizcaíno. La letrada señala que, cuando acaba la relación abogado cliente, los datos deberán seguir manteniéndose cifrados y conservados "con la única función de desencriptarlos ante posibles reclamaciones", añade.

Ambas expertas coinciden en que el plazo de conservación de los expedientes dependerá del tipo de datos tratados y la finalidad para la que se trataban, siendo el plazo de prescripción general de 5 años, ya que es el plazo en el que prescriben las acciones legales por responsabilidad civil.

Otras sanciones de la AEPD a despachos de abogados

A pesar de que, como hemos señalado, es la primera vez que la AEPD apercibe a un abogado por tirar documentos de sus clientes a la basura, desde la aprobación del RGPD el 25 de mayo de 2018, el organismo ha sancionado por vulnerar la normativa de protección de datos a varios profesionales de la abogacía.

Así, el 24 de noviembre de 2020, la AEPD sancionó con 10.000 euros (posteriormente reducidos a 6.000 euros por reconocimiento de culpa y pago voluntario) a un bufete por el envío de un correo electrónico a la parte reclamante, sin mantener en oculto al resto de destinatarios, revelando datos personales del afectado a terceros. No era la primera vez que la AEPD sancionaba este tipo de conductas, pues el 12 de diciembre de 2019 ya sanciono con

5.000 euros a otro despacho, quien además de revelar datos a terceros, realizó comunicaciones comerciales sin consentimiento de la parte reclamante.

El organismo también multó el 23 de octubre de 2020 con 1.600 euros a un abogado por el envío de un burofax por enviar un burofax en nombre de su cliente a una empresa en el que aparecían los datos personales de un tercero que no tenía ningún tipo de relación con la entidad que recibió la carta. Un caso bastante complejo en el que la AEDP acaba sancionando por infringir el artículo 6 del RGPD, al no contar la abogada remitente con base de legitimación para realizar el envío de los datos personales del tercero.

Por último, añadir la resolución de 6 de marzo de 2020, en la que se sanciona a una abogada que reutilizó documentos que contenían datos personales de antiguos clientes en el reverso, en concreto, para convocar a los inquilinos de un inmueble. Al igual que la conducta en la que el abogado tira documentos de sus clientes a la basura, la letrada vulneró el artículo 32 del Reglamento General de Protección de Datos (RGPD), que obliga a los responsables del tratamiento de datos a "aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado". Recibió 2.000 euros de sanción.