09/05/2025

Una práctica arraigada por una empresa que vulnera el RGPD: la AEPD sanciona el uso de WhatsApp personal para tratar datos de clientes

La reciente resolución de la Agencia Española de Protección de Datos (en adelante, AEPD) contra una asesoría vuelve a evidenciar que las prácticas normalizadas dentro de una organización no siempre se alinean con las exigencias normativas en materia de protección de datos. En este caso, la utilización de WhatsApp en el teléfono móvil personal de un empleado para enviar información relativa a clientes, pese a la oposición expresa del trabajador, ha motivado una sanción por vulneración de los artículos 6.1 y 32 del Reglamento General de Protección de Datos (en adelante, RGPD).

El asunto pone en cuestión una realidad muy extendida en pequeñas y medianas empresas: la informalidad en los canales de comunicación, la falta de control sobre los dispositivos personales y la creencia de que la costumbre o la eficiencia pueden justificar tratamientos de datos que no cumplen con las bases jurídicas ni con las garantías de seguridad exigidas por la normativa.

La reclamación, interpuesta por un trabajador de la empresa el 11 de agosto de 2023, se fundamentaba en el uso reiterado de su número personal de teléfono y su cuenta de WhatsApp como vía de comunicación para cuestiones laborales, particularmente para el envío de datos personales de clientes. Esta práctica se producía incluso tras múltiples advertencias por parte del trabajador en las que dejó constancia su disconformidad y pidió expresamente que no se utilizaran canales personales para cuestiones profesionales.

La documentación aportada por el reclamante incluía correos electrónicos, imágenes de conversaciones, y capturas de pantalla que evidenciaban el envío de archivos PDF con datos identificativos de clientes. La situación se mantuvo incluso después de que la relación laboral entre el trabajador y la empresa hubiera finalizado.

Por su parte, la empresa, en sus alegaciones, trató de justificar la utilización de WhatsApp personal apelando a razones históricas, funcionales y organizativas. Concretamente, alegó que:

- El uso de WhatsApp era una herramienta habitual en la empresa desde hacía décadas.
- Los trabajadores aceptaban voluntariamente esta vía por su rapidez y comodidad.
- La comunicación no se había producido fuera del horario laboral y ni se había vulnerado el derecho a la desconexión digital del empleado.
- El propio reclamante también había utilizado su número personal para cuestiones laborales, iniciando el mismo la conversación, lo cual demostraría una aceptación tácita.

Asimismo, sostuvo que no existía ninguna vulneración porque no se había difundido la información a terceros ni se había producido un perjuicio tangible para el trabajador o para los clientes cuyos datos fueron compartidos.

La AEPD, tras examinar los hechos aducidos por las partes, desestima las alegaciones de la empresa y constata, fundamentalmente, dos infracciones diferenciadas:

Infracción del artículo 6.1 del RGPD: licitud del tratamiento

El artículo 6.1 del RGPD establece que todo tratamiento de datos personales debe basarse en alguna de las condiciones de licitud contempladas en la norma: consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, protección de

intereses vitales, interés público o interés legítimo ponderado.

En este caso, la AEPD destaca que:

- No existía consentimiento explícito del trabajador para usar su teléfono personal, máxime cuando este lo había revocado de forma clara y reiterada.
- Una vez finalizada la relación laboral, la empresa carecía de base legal para continuar tratando los datos del extrabajador.
- No se había informado ni documentado debidamente ningún tipo de autorización sobre este tratamiento.

La Agencia recuerda, además, que el consentimiento debe ser libre, específico, informado e inequívoco (artículo 4.11 RGPD), y no puede presumirse por omisión ni por una supuesta aceptación derivada del uso informal o circunstancial del canal por parte del trabajador.

Asimismo, una vez finalizada la relación laboral, no existía ninguna de las causas previstas en el mencionado artículo 6.1 que justificase la licitud del tratamiento realizado por la entidad, ya que no existía un contrato laboral vigente ni se había obtenido el consentimiento de la parte reclamante para contactar con ella una vez finalizada la relación laboral.

Infracción del artículo 32 del RGPD: medidas de seguridad

El segundo eje de la resolución se centra en la infracción del deber de garantizar la seguridad del tratamiento. El artículo 32 del RGPD impone a los responsables la obligación de aplicar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, en función del riesgo que supone su tratamiento.

En este punto, la AEPD subraya que:

- El uso del dispositivo personal del trabajador para enviar datos de clientes a través de una aplicación como WhatsApp escapa al control de la empresa.
- La compañía no podía verificar si el teléfono del empleado contaba con cifrado, antivirus, políticas de bloqueo o limitación de acceso.
- No existía ninguna política interna de seguridad ni medidas específicas implementadas para mitigar el riesgo de acceso no autorizado o pérdida de información.

Además, destaca la gravedad de la reiteración, ya que el trabajador había advertido al menos en cuatro ocasiones de los riesgos asociados al uso de su número personal, sin que la empresa modificara su conducta.

La parte reclamada trató de motivar la reclamación como una represalia por parte del trabajador tras la extinción de la relación laboral, e incluso aludió a “móviles espurios” por parte del reclamante. Sin embargo, la Agencia deja claro que tales cuestiones, aun cuando existan, no desvirtúan los hechos probados ni las obligaciones legales de la empresa en materia de protección de datos.

Asimismo, se rechaza la justificación basada en la “costumbre inveterada”. La AEPD es contundente: ninguna práctica habitual puede eximir del cumplimiento del RGPD. El principio de responsabilidad proactiva (accountability) exige que las organizaciones se adapten a la normativa y sean capaces de demostrar su cumplimiento, con independencia de su tamaño o trayectoria.

Como resultado del procedimiento sancionador, la AEPD impone dos sanciones económicas a la empresa reclamada:

- 2.500 € por infracción del artículo 6.1 del RGPD, al tratar datos del trabajador (su número de teléfono personal) sin base jurídica una vez finalizada la relación laboral.
- 2.500 € por infracción del artículo 32 del RGPD, al no garantizar las medidas de seguridad necesarias al enviar datos personales de clientes a través de una aplicación no controlada por la empresa.

Para baremar la sanción, la autoridad de control parte del artículo 83.2 del RGPD y tiene en cuenta la naturaleza, gravedad y duración de la infracción, el alcance o propósito de la operación de tratamiento, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido. En este sentido, considera que el tratamiento de datos personales por el que se sanciona, que resulta de la utilización del número de teléfono particular de la parte reclamante, tuvo lugar en una única ocasión y

con la parte reclamante como única afectada.

No obstante, sí alega la circunstancia del artículo 76.2.b) de la Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales, entendida, en este caso, como circunstancia agravante: la vinculación de la actividad del infractor con la realización de tratamientos de datos personales. En este supuesto, la entidad, en el desarrollo de su actividad profesional necesita tratar de forma habitual datos personales, tanto de sus clientes como de sus propios trabajadores, lo que supone que tiene experiencia suficiente y debería contar con el adecuado conocimiento para el tratamiento de dichos datos.

Este caso evidencia, una vez más, la importancia de integrar la protección de datos en la cultura empresarial. Las herramientas tecnológicas no son neutras: su uso debe ir acompañado de un análisis legal, técnico y organizativo que garantice el cumplimiento normativo. No pueden dejarse al arbitrio de la costumbre, la conveniencia o la informalidad.

El uso de canales personales como WhatsApp o dispositivos no corporativos conlleva riesgos que deben gestionarse adecuadamente. En caso de optar por ellos (recordemos siempre con el consentimiento informado y documentado del trabajador), se deben aplicar políticas claras, medidas de seguridad robustas y sistemas de supervisión.

Finalmente, la resolución reafirma un pilar clave: el cumplimiento del RGPD no se puede relativizar por razones prácticas ni justificar por la ausencia de daño aparente. Basta con que se produzca un tratamiento de datos sin base legal o sin garantías suficientes para que exista una infracción sancionable.

Fuente: https://www.prodat.es/

LINK DE LA NOTICIA