El nuevo derecho a no recibir llamadas comerciales y su aplicación a la protección de datos

El pasado 29 de junio entró en vigor la modificación del artículo 66 de la Ley 11/2022 General de Telecomunicaciones, tras la cual se refuerza el derecho de los usuarios a no recibir llamadas comerciales no solicitadas. Así, la nueva redacción consagra el derecho de los usuarios a no recibir llamadas no deseadas con fines publicitarios, salvo que exista consentimiento previo del propio usuario para recibir este tipo de comunicaciones comerciales o salvo que la comunicación pueda ampararse en otra base de legitimación de las previstas en el Reglamento General de Protección de Datos. Esta obligación es aplicable de manera general a cualquier empresa o empresario que utilice estas prácticas y no solamente a las compañías de telecomunicaciones.

Hasta la entrada en vigor de la nueva redacción, las empresas podían realizar llamadas comerciales a todos los usuarios que no se hubiesen opuesto a ellas. Sin embargo, el cambio del paradigma normativo tiene como objetivo priorizar el derecho de los usuarios a no recibir llamadas publicitarias frente a los intereses comerciales de las empresas, aplicando así un criterio análogo al utilizado en la Ley 34/2002, de Servicios de la Sociedad de la Información en relación con los correos electrónicos publicitarios no solicitados (es decir, al denominado spam).

Debido a que el mencionado artículo 66 regula el derecho a la protección de datos personales en relación con las comunicaciones no solicitadas y con la finalidad de fijar su criterio, la Agencia Española de Protección de Datos ha publicado una circular que delimita su ámbito de aplicación. Las principales claves que otorga la Agencia en esta circular son las siguientes:

1. **El consentimiento como base legitimadora**. El consentimiento ha de otorgarse de conformidad con las exigencias del RGPD, de manera voluntaria, libre e informada. Este consentimiento será igualmente exigible cuando los usuarios figuren en las guías de abonados.

2. **Llamadas a números aleatorios**. Cuando las llamadas se realizan a través de la generación aleatoria de números de teléfono será igualmente exigible el consentimiento del usuario, por lo que se ponen límites a esta práctica habitual de las empresas de telemarketing.

3. **Interés legítimo del responsable**. Cuando la base legal del tratamiento sea el interés legítimo del responsable (o de un tercero), este deberá realizar previamente una ponderación entre los intereses del responsable y los derechos de los interesados. Esta ponderación deberá estar a disposición de la Agencia Española de Protección de Datos y ante los organismos de supervisión.

4. **Relación contractual previa**. Se presumirá lícito el tratamiento cuando el destinatario de las comunicaciones haya mantenido una relación contractual previa con el responsable durante el último año. Es decir, una empresa podrá realizar llamadas publicitarias a sus clientes, siempre que las comunicaciones se refieran a productos de su propia empresa similares a los que inicialmente contrató el usuario.

5. **Principio de transparencia**. Al inicio de la llamada, la empresa deberá informar sobre su identidad, indicar la finalidad comercial de la llamada e informar sobre la posibilidad de revocar el

consentimiento o ejercer el derecho de oposición a recibir llamadas comerciales no deseadas. Cualquier manifestación inequívoca del usuario contraria a la recepción de estas llamadas deberá entenderse como revocación del consentimiento.

6. **Grabación de la llamada**. Para demostrar el cumplimiento de la normativa de protección de datos, la empresa deberá proceder a la grabación de las llamadas comerciales.

La negligencia de un empleado ha motivado una sanción de 70.000 contra Vodafone

El pasado año 2022 una clienta de Vodafone interpuso una reclamación ante esta entidad tras ser víctima de un fraude. En concreto, el delincuente solicitó un duplicado de la tarjeta SIM de la reclamante y redirigió las llamadas entrantes, pudiendo acceder así a la información bancaria de la víctima y realizar una transferencia bancaria fraudulenta.

La reclamante, que recibió varios SMS de su banco informando de movimientos en su cuenta bancaria, pudo comprobar en la aplicación online de su banco que se había bloqueado su cuenta. Tras realizar las gestiones oportunas con Vodafone, esta compañía confirmó que había facilitado a un desconocido varón un duplicado de su tarjeta SIM, así como la desviación de la línea a otro teléfono. Al parecer, este varón se hizo pasar por una persona de confianza de la reclamante y únicamente se identificó con su nombre de pila, dando a continuación los datos de esta.

Vodafone alegó que la incidencia tuvo lugar porque el agente que llevó a cabo la contratación no siguió el procedimiento previsto en la política de seguridad para identificar debidamente al solicitante del trámite y asegurarse de que se trataba de la titular de la línea telefónica.

Manifiesta además que el agente, en contra del procedimiento previsto, no comprobó adecuadamente que el teléfono llamante no se correspondía con una línea telefónica a nombre de la reclamante ni verificó posteriormente la adecuación del trámite contactando a la numeración de la reclamante. En consecuencia, se incumplió la Política de Seguridad implementada por Vodafone y se actuó en contra de las directrices facilitadas por la entidad a sus agentes para la contratación de servicios mediante llamada telefónica.

Así, se puede determinar que el agente no cumplió el procedimiento implantado por Vodafone, que afirma que, de haberse cumplido, se hubiese denegado la solicitud del delincuente. Esta negligencia causó un tratamiento ilícito de los datos personales de la parte reclamante, lo que ha motivado una sanción contra Vodafone de 70.000 euros, que finalmente fue reducida a 56.000 euros por pago voluntario.

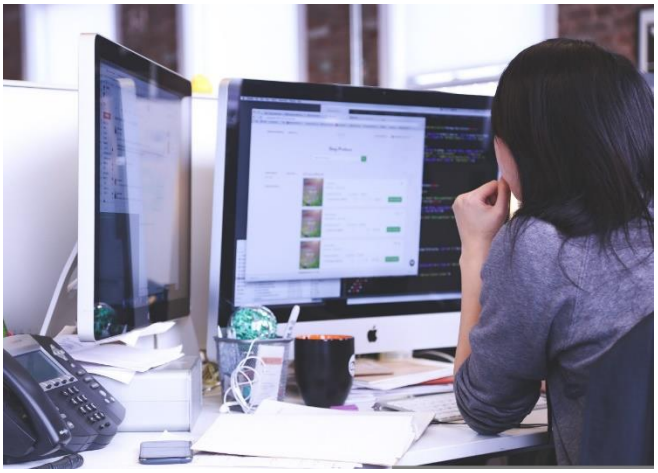
Esta resolución pone de manifiesto la necesidad de que las empresas se doten de protocolos para garantizar la licitud de los tratamientos de datos personales, así como de medidas técnicas y organizativas que garanticen el cumplimiento de estos protocolos.

Además, estas medidas deben de ir acompañadas de un protocolo para la formación y concienciación de los empleados en materia de seguridad y protección de datos, con la finalidad de que conozcan las medidas de seguridad a aplicar en su puesto de trabajo y crear así una cultura de protección de datos dentro de la organización.

Cinco claves para la seguridad en el puesto de trabajo

Un reciente estudio sitúa en una media del 14% el aumento de la inversión en seguridad informática en las empresas españolas, lo que pone en relieve la importancia que tiene la seguridad en una sociedad cada día más informatizada.

Sin embargo, la mayoría de las empresas descuida un aspecto esencial en la seguridad, que no es otro que la seguridad en el puesto de trabajo. Por esta razón, desde Microlab queremos trasladar las cinco claves necesarias para garantizar la seguridad en el puesto de trabajo:



1. Política de mesas limpias

El usuario debe mantener su puesto de trabajo ordenado, así como a guardar la documentación al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información, documentación o dispositivos extraíbles a la vista de personas no autorizadas que pudieran hacer un uso indebido de la misma. También se deben evitar prácticas como la de apuntar contraseñas en post-it o papeles.

Además, se debe bloquear el ordenador al ausentarse del puesto de trabajo, de modo que no quede accesible para cualquier persona, y apagar el equipo de trabajo al finalizar la jornada laboral.

2. Programar el bloqueo de sesión y configuración del equipo

El personal informático deberá programar un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo.

Además, el trabajador no debe tener la capacidad de modificar la configuración del equipo ni de instalar programas o aplicaciones por su propia iniciativa. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.

3. Uso de impresoras y escáneres

El usuario debe recoger inmediatamente aquellos documentos enviados a imprimir y guardar la documentación una vez escaneada. Este tiene la obligación de custodiar la información expuesta en impresoras y escáneres.

4. Navegación por internet

Durante la navegación por internet el empleado debe verificar que las direcciones (URL) de destino son correctas y que el certificado es válido cuando se trate de conexiones a entornos seguros o se realicen transacciones. Además, deberá comprobar que se cumple el protocolo https:// en las páginas donde se trabaje con información de la empresa.

5. Destrucción de la documentación

La documentación obsoleta o aquella cuyo tratamiento ya no sea necesario se destruirá de forma segura, de forma que se garantice la irrecuperabilidad de la información. En particular, se deberá utilizar la destructora de papel o el servicio de destrucción de documentos puesto a disposición del empleado. Únicamente se deberá imprimir documentación cuando sea estrictamente necesario para el desarrollo del trabajo.

6. Formación de protección de datos

Los empleados con acceso a datos personales deben conocer los riesgos que puedan surgir en el desarrollo de su trabajo, así como las instrucciones que deben seguir en caso de incidente durante el tratamiento.

Es importante generar una cultura de la privacidad en la organización y que los empleados estén formados y sepan actuar en caso de sufrir un ataque informático, fugas de información o ejercicio de derecho de algún cliente.

Editado por Microlab Hard

Madrid. C/ Cronos 8, 1º, Madrid

Barcelona. C/ Santiago Rusiñol 8, Molins de Rei