Robo de datos de clientes: 3 claves para proteger tu negocio

¿Te preocupa el **robo de datos de clientes**? Un empleado se marcha de tu empresa y se lleva toda tu base de datos con los datos de tus clientes.

¿Qué puede pasar?

Aunque sea una situación que hemos normalizado, lo cierto es que no solo compromete tu cuenta de resultados, también te expone a una **sanción monumental** de la Agencia Española de Protección de Datos si no has sabido anticipar adecuadamente esta situación y prevenirla.

Tu responsabilidad con los datos de tus clientes

Cuando pones a disposición de un empleado información de clientes, una cuenta de correo de correo electrónico y soportes informáticos que almacenan esta información, estás también comprometiendo la **seguridad y reputación** de tu negocio si no tomas las medidas adecuadas para garantizar un **uso responsable por parte de tu empleado**.

¿Te lo has planteado alguna vez?

Es posible que no.

Imagina esta escena:

Primer acto: Un empleado se marcha de tu empresa con una copia de la base de datos de tus clientes para poder utilizarlos posteriormente o comercializar con ellos.

Segundo acto: uno de estos clientes presenta una denuncia a la Agencia de Protección de Datos tras el envío de correos electrónicos publicitarios por parte de este ex trabajador sin su consentimiento.

Tercer acto: Se abre un expediente sancionador donde se descubre el origen de la información y se te exigen responsabilidades a ti por incumplir con el deber de secreto al que estás obligado.

Tu pagas los platos rotos

La Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD) expresa en el artículo 10 el **deber de secreto profesional** expresando de esta manera:

*"El responsable del fichero y **quienes intervengan en cualquier fase del tratamiento** de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, **obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero** o, en su caso, con el responsable del mismo".*

*"El incumplimiento del deber de secreto constituye **infracción grave** de acuerdo con lo previsto en el artículo 44.3.d) de la LOPD: 'La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley'."*

Queda claro que no es ninguna tontería el exponer tu negocio a una infracción grave que puede suponer una sanción de hasta 600.000 €

La importancia del deber de secreto

El deber de secreto es la principal obligación y responsabilidad de las empresas frente al dato personal.

- Gracias al secreto, garantizas a las personas la soberanía sobre su propia información y la potestad de decidir sobre su uso y destino.
- Aseguras también que no revelarás esa información a ninguna persona o entidad ajena a tu negocio, fuera de los casos autorizados por la Ley.

Por tanto, la **sustracción de tu base de datos** por parte de un empleado, vulnera la obligación de secreto respecto a tus clientes y te expone a una sanción tipificada como **grave.**

Además que la ley especifica que esta obligación **subsistirá** aun después de finalizar sus relaciones con el titular del fichero.

A menos que…

- Hayas informado de manera clara a tu empleado de su obligación al secreto respecto a los datos de tus clientes.
- Le hayas requerido su conformidad y compromiso con esta obligación.
- Puedas acreditar ambas cosas.

Informar adecuadamente es la clave

Una de las reglas básicas para **prevenir y proteger** tu negocio es la de **informar adecuadamente** a tu o tus trabajadores sobre este deber de secreto y su responsabilidad frente a la información a la que tienen acceso y los soportes que la almacenan.

¿Cómo lo haces?

3 claves para proteger tu negocio del robo de datos de clientes

1. **Mediante un escrito** donde expongas de manera comprensible el deber de secreto al que están obligados respecto a la información personal a la que tienen acceso en el ejercicio de sus funciones. Deberás advertir también en ese escrito que estas obligaciones **subsistirán** una vez finalizada la relación laboral y que devolverán inmediatamente cualquier soporte o documento en el que conste información de carácter personal fruto de su actividad laboral en tu empresa.

2. Recogiendo el **consentimiento firmado** de tus empleados donde manifiesten su conformidad con los términos expuestos, conocen sus obligaciones y se comprometen a cumplirlas.
3. Una **charla informativa** para aclarar estos términos y acreditar el conocimiento completo de sus obligaciones.

La **ausencia de un documento** que acredite la información previa y en **consentimiento** por parte de tus empleados compromete seriamente el futuro de tu negocio. Aprende a prevenir y a blindarte legalmente frente al robo de base de datos.

Recuerda:

Ante una denuncia, **siempre será la empresa quien responda de las responsabilidades derivadas del incumplimiento del deber de secreto.**

En este sentido, la Agencia Española de Protección de datos lo deja bien clarito:

No se debe caer en el error de considerar como responsable de las infracciones en materia de Protección de Datos directamente **al personal de la empresa, siendo que en caso de comisión de una infracción la responsabilidad y sanciones se imputan a la empresa**.

Pero además, según el art. 1903.4 del **Código Civil**: “Son responsables los dueños o directores de un establecimiento o empresa, respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones”.

El 120.4 del **Código Penal** dice que son también responsables civilmente las personas naturales o jurídicas de cualquier género de industria o comercio por delito o falta que hayan cometido sus empleados o dependientes, representantes o gestores en la ejecución de sus obligaciones o servicios.

Y esto porque…

Es la empresa quien tiene que adoptar las medidas internas necesarias para la reducción o **minimización del riesgo** y en el caso del deber de secreto, la mejor manera de hacerlo es:

- **Formar**, para crear conciencia sobre el dato personal como bien jurídico.
- **Informar**, sobre la responsabilidad que conlleva el tratamiento de datos personales.
- **Requerir consentimiento explícito y voluntario,** para acreditar el cumplimiento de la empresa con ambas obligaciones y derivar responsabilidades.

Prevenir, siempre más efectivo que lamentar

Si te has asegurado de realizar esas tres tareas, tendrás la posibilidad de probar **la responsabilidad directa de tu empleado frente a la infracción y podrás** ejercer las acciones disciplinarias y legales que correspondan.

Por eso, nada más producirse la contratación debes:

1. **Definir los datos a tratar** por parte de empleados, establecer las medidas de seguridad y las obligaciones que vas exigir respecto a la información personal a que tendrán acceso tus empleados.
2. **Disponer de impresos** de modelos anexos al contrato con estos términos.
3. **Recoger y archivar** adecuadamente estos impresos debidamente firmados por tus empleados.