LISTA DE CONTROL DEL CUMPLIMENTO DEL RGPD: 10 MEDIDAS QUE DEBES TOMAR:

Aviso legal: es importante enfatizar que, a pesar de poner en práctica esta lista de acciones, Centraliza no garantiza que una compañía esté cumpliendo la ley de privacidad al 100 %. Centraliza ofrece únicamente algunos consejos y recomendaciones sobre el RGPD. Este contenido fue redactado con fines informativos y no debe ser interpretado como un asesoramiento legal ni utilizado para determinar cómo el RGPD podría aplicarse a ti y a tu empresa.

Check

- **1.** Realiza **auditorías internas** en tus flujos de datos para mapearlos y ver qué necesita ajustarse al nuevo Reglamento. Además, **analiza y actualiza todos tus documentos legales**.

- **2.** Consigue el **permiso** explícito para el procesamiento de datos: comprueba cómo lo haces actualmente. Pide consentimiento de nuevo si el que tienes no cumple con lo establecido en el RGPD (mira cómo solicitar el consentimiento en el capítulo 1 de este e-book).

- **3.** Comunica a tus clientes **cómo y por qué recopilas datos y explícales por cuánto tiempo planeas almacenar sus datos** en una declaración de privacidad[2]. Para ayudarte a prepararte para esto, puedes organizar una auditoría de información para mapear qué datos almacenas, de dónde vienen y con quién los compartes. Además, informa a tus empleados y actualiza los documentos y procedimientos para uso interno (por ejemplo, portátiles, redes sociales y política de privacidad, contratos de empleados, reglamentos laborales).

- **4.** Forma a tus empleados y crea concienciación mediante sesiones informativas para entender cómo os afectará el RGPD.

- **5.** Muestra **evidencia** del cumplimiento de la normativa: identifica la base legal para tu actividad de procesamiento en el RGPD, documenta tus procedimientos y actualiza tu aviso de privacidad para explicarlo. Por ejemplo, modifica tus "Términos y condiciones" y/o el acuerdo cerrado con tus clientes. Además, cierra un acuerdo de procesamiento de datos (APD) con procesadores de datos y, en su caso, con subprocesadores también.

- **6.** Dispón de un sistema para **eliminar** los datos personales una vez haya finalizado el período de retención legal o cuando los interesados lo soliciten.

- **7.** Crea un **plan de gestión de crisis** claro y detallado en caso de que haya que detectar, informar e investigar una violación de datos. Nota importante: según el tipo de incidente o violación, es obligatorio informar dentro de un plazo establecido.

  Para más información sobre cuándo y en qué plazo informar de una crisis, consulta a tu Autoridad de Protección de Datos nacional.

- **8.** Actualiza o crea los **procedimientos de acceso**: por ejemplo, tus servidores deben ser inaccesibles para todo aquel que no esté autorizado. En cambio, los interesados deben poder acceder a sus propios datos siempre que lo soliciten.

- **9.** Protección de datos para **menores de 16 años**, necesitan el permiso del padre, la madre o un tutor. Los países de la UE podrán establecer una edad inferior, siempre que no sea inferior a 13 años. Bélgica y Francia, por ejemplo, modificarán esta edad a los 13 años.

- **10.** Designa un **Oficial de Protección de Datos (OPD)** para supervisar tu estrategia y cumplimiento del programa. Si bien esto no es obligatorio para todas las empresas, sí es recomendable. Un OPD puede ser un consultor externo o un trabajador que asuma ese papel extra además de sus responsabilidades diarias.

[2] Una declaración de privacidad debe referirse, al menos, al RGPD y contener información sobre qué datos personales recopilas, cómo lo haces, el propósito del procesamiento, el período de retención de los datos, los derechos del interesado, el procedimiento de queja, el proceso de trasferencia a terceros, etc.