SAPIENSDATAAI
Agentes IA conversacionales · contacto@sapiensdataai.es

Cómo usar IA con datos de tus clientes sin meterte en líos legales

Guía para pymes que quieren implementar IA — escrita en lenguaje de verdad

Elaborada por: SAPIENSDATAAI · contacto@sapiensdataai.es
Revisión recomendada: cada 6 meses o ante cambio normativo.

> ⚠ **AVISO IMPORTANTE — LEER ANTES DE NADA**
> Esta es una guía **ORIENTATIVA e INFORMATIVA**. Es una **recopilación de la normativa vigente** que vamos investigando y de **cómo, a nuestro criterio, creemos que se adapta a las pymes** que quieren implementar inteligencia artificial.
> **SAPIENSDATAAI NO garantiza** que la información sea exhaustiva, esté totalmente actualizada, ni sea jurídicamente exacta al 100%, y **NO se hace responsable** de las decisiones que se tomen basándose en ella ni de la veracidad o vigencia de los datos aquí recogidos.
> Este documento **NO constituye asesoramiento jurídico** ni sustituye la consulta con un abogado especializado en protección de datos. Antes de tomar decisiones vinculantes (firmar contratos/DPA, desplegar sistemas con datos sensibles), **validar siempre con un profesional del derecho.**

---

1. PARA QUÉ SIRVE ESTA GUÍA

Estáis pensando en usar una IA para gestionar información de vuestros clientes. Puede ser para responder consultas, buscar en documentos, analizar expedientes... lo que sea.

Bien. Pero hay algo que debéis saber desde el principio: **usar IA con datos de personas implica cumplir unas obligaciones legales muy concretas**. No es suficiente con que el cliente haya dicho que sí.

Esta guía os explica, sin rodeos ni jerga innecesaria:
- Qué leyes aplican y qué os obligan a hacer.
- Qué datos hay que proteger antes de que la IA los toque, y cuánto.
- Qué pasos tenéis que dar para hacerlo bien.

El objetivo es que podáis implementar la IA con tranquilidad, sabiendo qué hace falta y cuándo.

⚠ LO MÁS IMPORTANTE — LEED ESTO BIEN: "TENEMOS EL CONSENTIMIENTO DEL CLIENTE, ASÍ QUE PODEMOS METER SUS DATOS EN UNA IA SIN PROBLEMA" → ESO ES FALSO

Este es el error más frecuente. Y conviene tenerlo clarísimo desde el principio.

El consentimiento del cliente os permite tratar ese dato (usarlo, guardarlo, procesarlo). **Pero no os autoriza a enviárselo en bruto a una IA.** Y tampoco os libra de hacer estas otras cosas, que son obligatorias por separado — cada una viene de una ley distinta:

A continuación, una tabla con las creencias más comunes y lo que la ley dice de verdad:

Lo que se suele creer	Lo que de verdad exige la ley	Norma
"Tengo el consentimiento → mando el dato tal cual a la IA"	El consentimiento es solo la **base legal** para poder tratar el dato. Pero aparte, tenéis que **protegerlo** (seudonimizar + cifrar) según el riesgo — y esto es obligatorio aunque el cliente haya dicho que sí	**Art.32 RGPD**
"Si el cliente acepta, uso cualquier proveedor de IA"	Necesitáis un **contrato firmado** (lo que se llama DPA, que es simplemente un contrato con el proveedor) con cada empresa que toque vuestros datos. El consentimiento del cliente no crea ese contrato	**Art.28 RGPD**
"El consentimiento cubre que la IA esté en EE.UU."	No. Si la IA procesa datos en servidores fuera de Europa, hacen falta **unas garantías adicionales** (Cláusulas Contractuales Tipo + Evaluación de Transferencia). El consentimiento no llega para eso	**Schrems II + Arts.44-49 RGPD**
"Con el consentimiento proceso datos de salud sin problema"	Para datos de salud hay un paso extra obligatorio: una **evaluación de impacto** (DPIA, que es un análisis previo de los riesgos) antes de arrancar, y los datos **nunca pueden llegar en bruto a la IA**	**Art.9 + Art.35 RGPD**
"Si consiente, mando todos sus datos"	Solo podéis tratar lo **necesario**. Si la IA puede hacer su trabajo con datos protegidos, mandar el dato real en claro **incumple la ley** aunque el cliente haya consentido	**Art.5.1.c RGPD**

Resumiendo: el consentimiento abre la puerta a usar el dato. Pero **la IA nunca debe ver el dato sensible tal cual**. Antes hay que protegerlo, firmar el contrato con el proveedor, hacer el análisis de riesgos si aplica, y cubrir las garantías si los servidores están fuera de Europa.

Fuente: AEPD — Guía adecuación RGPD a IA.

---

2. LAS LEYES QUE APLICAN

2.1 RGPD — La ley europea de protección de datos (Reglamento UE 2016/679)

Vigente desde 2018. Si vuestra empresa trata datos de personas, sois **Responsables del Tratamiento** — es decir, vosotros respondéis de que todo se haga bien.

Qué os obliga a hacer:
- Tener una **razón legal** (lo que se llama base legal) para cada dato que uséis.
- Aplicar **medidas de seguridad** proporcionales al riesgo: proteger los datos, cifrarlos, controlar quién accede (Art.32).
- Respetar los **derechos ARCO** de vuestros clientes: que puedan acceder a sus datos, corregirlos, borrarlos o pedir que no los uséis.
- Firmar un **DPA** (contrato de encargado) con cada proveedor externo que maneje datos en vuestro nombre.
- Llevar un **registro** de qué datos uséis y para qué.

Sanciones: hasta 20 millones de euros o el 4% de vuestra facturación mundial anual (Art.83.5). Se aplica el importe mayor.

Fuente: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

2.2 LOPDGDD — La adaptación española del RGPD (LO 3/2018)

Es el RGPD aplicado a España. La **AEPD** (Agencia Española de Protección de Datos) es quien manda aquí — es la que investiga y sanciona.

2.3 EU AI Act — La ley que regula la inteligencia artificial (Reglamento UE 2024/1689)

La primera ley del mundo que regula específicamente la IA. Clasifica los sistemas de IA por niveles de riesgo.

Obligación universal desde el 02/08/2026 (Art.50): cualquier asistente de IA que hable con personas tiene que incluir un **aviso visible de que es una IA**. Sin ese aviso, estáis incumpliendo la ley. Quedan pocos meses.

Sanciones (Art.99) — hay tres niveles:
- **Hasta 35 M€ o 7%** de facturación → solo por prácticas prohibidas expresamente (Art.5). La mayoría de pymes no llega aquí.
- **Hasta 15 M€ o 3%** → por no poner el aviso de IA o incumplir las obligaciones de alto riesgo. **Este es el tramo que os puede afectar.**

- **Hasta 7,5 M€ o 1%** → por dar información incorrecta a las autoridades.
- **PYME o startup:** se aplica siempre el importe menor de los dos (el porcentaje o la cifra fija), no el mayor.

Fuente: https://artificialintelligenceact.eu/article/99/ | Anexo III (alto riesgo): https://artificialintelligenceact.eu/annex/3/

2.4 Normativa del vuestro sector

Según lo que hagáis (sanidad, seguros, banca, legal...) puede haber leyes adicionales.

Y un detalle importante sobre los **datos especiales** (datos de salud, religión, origen étnico, etc.): el Art.9 del RGPD **no acepta "ejecución del contrato" como razón para tratarlos** — eso solo vale para datos normales (Art.6). Para datos especiales, las razones legales válidas son: **consentimiento explícito del interesado (Art.9.2.a)**, **interés público con habilitación legal del sector (Art.9.2.g)** o **gestión de reclamaciones legales (Art.9.2.f)**. Consultad con vuestro asesor cuál aplica a cada caso.

2.5 Schrems II — Cuando la IA tiene los servidores fuera de Europa

Si el modelo de IA que uséis procesa datos **fuera del Espacio Económico Europeo** (que incluye la UE más Noruega, Islandia y Liechtenstein) — lo habitual con proveedores de EE.UU. — necesitáis dos cosas: **Cláusulas Contractuales Tipo (CCT)** firmadas con ese proveedor, más una **Evaluación de Impacto de la Transferencia (TIA)**. El consentimiento del cliente no cubre esto. La AEPD ha sancionado por enviar datos a EE.UU. sin estas garantías.

---

3. TABLA: SEGÚN EL TIPO DE DATO, CUÁNTA PROTECCIÓN NECESITA ANTES DE LLEGAR A LA IA

Antes de ver la tabla, aquí van las definiciones de los niveles, de mayor a menor exigencia:

- **PROHIBIDO EN CLARO** = el dato real nunca puede llegar al modelo de IA. Es obligatorio sustituirlo por un código antes. Como si quitarais el nombre de un expediente y pusierais un número — la IA trabaja con el número, no con el nombre.
- **SEUDONIMIZACIÓN** = sustituir el dato por un código recuperable. Es como cambiar el nombre real por un mote: la IA ve el mote, y solo vosotros sabéis quién es de verdad. El RGPD sigue aplicando porque vosotros podéis revertirlo.
- **MINIMIZACIÓN** = enviar solo lo imprescindible y quitar o sustituir los identificadores.
- **NINGUNO** = puede usarse en claro (porque no es un dato personal o ya está anonimizado de forma irreversible — como borrar el mote y la lista, ya no hay forma de saber quién era).

Esta tabla resume qué hacer con cada tipo de dato:

Tipo de dato	Nivel de protección exigido	Qué hay que hacer	Norma
Datos de SALUD (diagnósticos, lesiones, historial clínico, discapacidad, bajas)	🔴 **PROHIBIDO EN CLARO** (categoría especial)	Sustituir por código + cifrado AES-256 + guardar la clave en Europa + **evaluación de impacto previa obligatoria** (DPIA)	Art.9 + Art.32 + Art.35 RGPD
Otros datos especiales (origen étnico, religión, ideología, orientación sexual, datos genéticos y biométricos)	🔴 **PROHIBIDO EN CLARO**	Igual que los datos de salud	Art.9 RGPD
Datos identificativos (nombre, NIF/NIE, dirección, email, teléfono, matrícula)	🟠 **SEUDONIMIZACIÓN**	Sustituir por un código interno antes de enviarlo a la IA; solo el personal autorizado puede recuperar el dato real	Art.6 + Art.32 RGPD
Datos económicos y bancarios (IBAN, tarjeta, importes sensibles)	🟠 **SEUDONIMIZACIÓN / enmascarado**	Sustituir IBAN y tarjeta por código; ocultar importes si no son imprescindibles para la respuesta	Art.32 + Art.5.1.f RGPD
Identificadores indirectos (número de cliente, expediente, contrato, póliza, historia clínica)	🟠 **SEUDONIMIZACIÓN**	Sustituir por una referencia interna	Art.32 + Recital 26 RGPD
Datos personales no sensibles para la tarea (descripción de un caso sin identificar a la persona)	🟡 **MINIMIZACIÓN + sustituir el identificador**	Enviar solo lo necesario; quitar o codificar quién es	Art.5.1.c RGPD
Contenido que no es personal (documentación técnica, normativa, procedimientos, FAQ, condiciones)	🟢 **NINGUNO** (en claro)	Verificar que no haya datos personales escondidos	—
Estadísticas o datos agregados anónimos (irreversibles)	🟢 **NINGUNO** (fuera del RGPD)	Verificar que la anonimización es de verdad irreversible	Recital 26 RGPD

Regla de oro: ante la duda sobre si un dato es sensible, tratadle como si lo fuera (seudonimizadlo). Y recordad: la seudonimización es reversible — el RGPD sigue aplicando aunque el riesgo se reduzca mucho.

---

4. SI EL CLIENTE CONSIENTE, ¿HAY QUE PROTEGER IGUALMENTE LOS DATOS?

Sí. Siempre. El consentimiento no es un salvoconducto de seguridad.

El consentimiento os permite usar el dato. Pero no elimina ninguna de estas obligaciones — son acumulativas, cada una viene de una norma distinta:

1. **Medidas de seguridad (Art.32):** seudonimización y cifrado según el riesgo, con independencia del consentimiento. Para datos de salud, es obligatorio sin excepciones.
2. **Garantías de transferencia internacional (Schrems II):** si la IA procesa fuera de Europa, hacen falta CCT + TIA aunque el cliente haya firmado cualquier cosa.
3. **DPA con el proveedor de IA (Art.28):** el proveedor del modelo es vuestro encargado del tratamiento. Necesitáis un contrato firmado con ellos — el consentimiento del cliente no lo crea.
4. **DPIA — evaluación de impacto (Art.35):** obligatoria si tratáis datos de salud (u otros de alto riesgo) de forma habitual. Hay que hacerla antes de arrancar, no después.
5. **Minimización (Art.5.1.c):** aunque el cliente consienta, solo tratáis lo necesario. Si la IA puede responder con datos protegidos, mandar el dato real en claro incumple la ley.

---

5. PASOS A SEGUIR (CHECKLIST)

Lo que tenéis que hacer vosotros (empresa)

- [ ] **Identificar y clasificar** qué datos vais a tratar con IA y dónde cae cada uno en la tabla de la sección 3.

- [ ] **Documentar la base legal** de cada tratamiento. Para datos normales: Art.6. Para datos especiales: Art.9.2.a, 9.2.f o 9.2.g — confirmad con vuestro asesor.
- [ ] **Firmar un DPA (Art.28)** con cada proveedor que vaya a tocar vuestros datos (proveedor del modelo de IA, base de datos, hosting).
- [ ] **CCT + TIA (Schrems II)** si algún proveedor procesa datos fuera de Europa.
- [ ] **DPIA (Art.35)** si tratáis datos de salud u otros de alto riesgo de forma habitual — hacerla **antes** de arrancar.
- [ ] **Actualizar la política de privacidad y el aviso legal** (Arts.13/14): informar a los clientes de que se usa IA y qué proveedores intervienen.
- [ ] **Actualizar el Registro de Actividades de Tratamiento (Art.30).**
- [ ] **Poner el aviso visible "Este asistente usa inteligencia artificial"** (EU AI Act Art.50) — obligatorio antes del **02/08/2026**.
- [ ] **Consultar al DPO** (Delegado de Protección de Datos) si lo tenéis, o valorar si estáis obligados a tenerlo, antes de arrancar con datos sensibles.
- [ ] **Supervisión humana:** la IA sugiere, pero las decisiones que afectan a los derechos del cliente las toma siempre una persona.

Lo que hace el proveedor de IA técnico (implementado por nosotros)

- [ ] **Proteger los datos antes del modelo:** sustituir los datos sensibles por códigos internos antes de que la IA los vea, según la tabla de la sección 3.
- [ ] **Vault cifrado (AES-256) en Europa:** la tabla que relaciona código con dato real se guarda cifrada en un servidor europeo. La clave nunca sale de Europa.
- [ ] **Control de acceso por rol:** solo el personal autorizado puede recuperar el dato real. Quedan registros de quién accede.
- [ ] **Retención de logs limitada** (máximo 6 meses) con borrado automático.
- [ ] **Función de supresión de datos:** para cuando un cliente ejerza su derecho de borrado (Art.17 RGPD).
- [ ] **Aviso de IA** en la interfaz desde el primer mensaje.

---

6. QUIÉN RESPONDE DE QUÉ

Esta tabla aclara los dos roles que establece la ley:

Rol	Quién es	Qué responsabilidad asume
Responsable del Tratamiento	Vuestra empresa	Vosotros decidís para qué se usan los datos. Respondéis ante vuestros clientes y ante la AEPD. Firmáis los DPA. **Si hay una sanción, os llega a vosotros.** Esta responsabilidad no se puede traspasar a nadie.
Encargado del Tratamiento	El proveedor de IA (p.ej. SAPIENSDATAAI)	Trata los datos **solo según vuestras instrucciones**. No puede usarlos para sus propios fines. Implementa las medidas técnicas acordadas en el DPA. Indica qué subproveedores usa (modelo de IA, base de datos, hosting).

---

7. CÓMO FUNCIONA LA PROTECCIÓN TÉCNICA

Os explicamos cómo funciona el sistema que aplicamos, con un ejemplo concreto:

1. Antes de la IA, sustituimos los datos reales por códigos.
Antes de que cualquier dato llegue al modelo de IA, el sistema lo convierte en un código. Por ejemplo: "Juan García" se convierte en `CLIENTE_REF_001`, y "diabetes" en `CONDICION_SALUD_A`. El modelo trabaja con esos códigos. **Nunca ve el dato real.**

2. La tabla código↔dato real se guarda cifrada en Europa.
Esa tabla (la que dice que `CLIENTE_REF_001` es Juan García) se guarda cifrada en un servidor dentro de la Unión Europea, bajo vuestro control. El modelo de IA no tiene acceso. La clave de descifrado nunca sale de Europa.

3. Al mostrar la respuesta, recuperamos el dato real.
Cuando un empleado vuestro lee la respuesta del asistente, el sistema sustituye los códigos por los datos reales. El empleado ve "Juan García". El modelo nunca lo procesó en claro.

Lo que cubre: reduce mucho el riesgo de que el proveedor del modelo vea datos sensibles, y facilita cumplir el Art.32.

Lo que NO elimina: el DPA, la DPIA, las garantías de transferencia y la política de privacidad. Seguís necesitando todo eso, porque los datos protegidos por código (seudonimizados) siguen siendo datos personales según el RGPD (Art.4.5 / Recital 26) — vosotros podéis revertirlos.

No prometemos que ningún sistema sea invulnerable. Aplicamos las medidas del estado del arte y actuamos como encargados responsables (Art.28 RGPD).

---

8. GLOSARIO — LAS PALABRAS QUE APARECEN EN ESTA GUÍA

Término	Qué significa en lenguaje normal
RGPD / LOPDGDD	La ley europea (UE 2016/679) y española (LO 3/2018) de protección de datos.
EU AI Act	La ley de la UE que regula la IA por niveles de riesgo (Reglamento UE 2024/1689). Fecha clave: 02/08/2026.
AEPD	La Agencia Española de Protección de Datos. Es quien puede sancionaros en España.
Categoría especial (Art.9)	Los datos que tienen la máxima protección por ley: salud, origen étnico, religión, ideología, orientación sexual, datos genéticos y biométricos.
DPA	Contrato de Encargado del Tratamiento (Art.28). Es el contrato que tenéis que firmar con cada proveedor que maneje vuestros datos.
DPIA	Evaluación de Impacto de Privacidad (Art.35). Un análisis de riesgos que hay que hacer antes de arrancar sistemas que traten datos de alto riesgo (como datos de salud).
DPO	Delegado de Protección de Datos. La persona (o empresa externa) que supervisa que cumpláis el RGPD.
Seudonimización	Sustituir datos por códigos que se pueden revertir. Como cambiar el nombre por un mote: la IA ve el mote, vosotros sabéis quién es. El RGPD sigue aplicando.
Anonimización	Borrar los datos de forma irreversible. Como quemar la lista de quién es quién — ya no hay forma de saberlo. Entonces sale del RGPD (Recital 26).
CCT / TIA	Cláusulas Contractuales Tipo y Evaluación de Impacto de la Transferencia. Son los documentos que necesitáis para enviar datos a servidores fuera de Europa.
Schrems II	Una sentencia del Tribunal de Justicia de la UE que obliga a usar CCT + TIA cuando vuestros datos van a servidores en EE.UU.
Art.50 EU AI Act	La obligación de avisar a los usuarios de que están hablando con una IA. Obligatorio desde el 02/08/2026.

---

9. FUENTES OFICIALES

Fuente	URL
RGPD (EUR-Lex)	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
EU AI Act — Art.50 transparencia	https://artificialintelligenceact.eu/article/50/
EU AI Act — Art.99 sanciones	https://artificialintelligenceact.eu/article/99/
EU AI Act — Anexo III alto riesgo	https://artificialintelligenceact.eu/annex/3/
AEPD — Guía Adecuación RGPD a IA	https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf
AEPD — Art.32 seguridad	https://lexparency.es/eu/RGPD/ART_32/
Schrems II / transferencias (TJUE C-311/18)	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62018CJ0311

Elaborado por SAPIENSDATAAI — contacto@sapiensdataai.es
Guía ORIENTATIVA e INFORMATIVA: recopilación de normativa vigente y de cómo creemos que se adapta a las pymes que implementan IA. SAPIENSDATAAI NO garantiza su exactitud, exhaustividad ni vigencia, y NO se responsabiliza de las decisiones tomadas en base a ella. NO sustituye asesoramiento jurídico. Validación de un abogado obligatoria antes de firmar DPA o go-live con datos sensibles.