Lista de comprobación de RGPD y Reglamento de IA para activar un agente de IA

Lo que va entre corchetes se sustituye por los datos de la empresa. Cada casilla [ ] se marca solo con una respuesta escrita y un documento que la respalde.

EMPRESA
[Nombre de la empresa]

PROVEEDOR
[Nombre del proveedor]

REUNIÓN
[fecha]

ASISTEN
[soporte, legal y protección de datos]

LA LISTA, EN CIFRAS

13	8	3	2 ago 2026
Apartados con casillas	Respuestas por escrito	Columnas en el registro	Aviso de IA exigible

00 Datos de la reunión

Empresa responsable [Nombre de la empresa]. Proveedor del agente de IA [Nombre del proveedor]. Proveedor del modelo de lenguaje [Nombre, si es distinto]. Canales donde atenderá el agente [chat, correo, WhatsApp]. Fecha [fecha]. Asistentes de legal, seguridad, soporte y dirección [nombres].

Datos que el agente verá [nombre, correo, teléfono, contenido de las conversaciones, adjuntos, datos de cuenta, otros]. Si entre ellos hay datos de salud u otras categorías especiales, se rellena también el apartado 11.

01 Base jurídica y finalidades

☐ La atención con IA figura en el registro de actividades de tratamiento, como tratamiento propio o dentro del de atención al cliente.

☐ Cada finalidad tiene su base jurídica anotada. Atender a clientes con contrato suele apoyarse en la ejecución del contrato, y a quien aún no lo es, en medidas precontractuales o en el interés legítimo.

☐ Cualquier otro uso de las conversaciones, como entrenar modelos o elaborar perfiles, tiene su propia base y no se da por incluido en la atención.

02 Deber de informar y aviso de IA

☐ La política de privacidad dice que parte de la atención la presta un sistema de IA, qué datos trata y qué terceros intervienen.

☐ El agente se presenta como una IA en el primer mensaje, en todos los canales donde atiende.

☐ Si la empresa atiende en varios idiomas, el aviso existe en cada uno.

☐ Hay un camino visible para hablar con una persona.

☐ El equipo que opera el agente tiene formación en IA suficiente para usarlo y supervisarlo. La alfabetización en IA está en el artículo 4 del Reglamento de IA, que se aplica desde el 2 de febrero de 2025.

03 Contrato de encargado

☐ Hay un contrato firmado con el proveedor, con objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos y categorías de personas.

☐ El proveedor trata los datos solo con instrucciones documentadas de la empresa.

☐ Las personas autorizadas del proveedor están sujetas a confidencialidad.

☐ Las medidas de seguridad están descritas en el contrato.

☐ El proveedor ayuda a atender los derechos de las personas y a hacer evaluaciones de impacto cuando proceda.

☐ Al terminar, el proveedor suprime o devuelve los datos, a elección de la empresa, incluidas las copias.

☐ La empresa puede pedir información y auditar al proveedor.

☐ El proveedor avisa a la empresa si cree que una instrucción infringe la normativa.

04 Dónde se procesan los datos

☐ Consta por escrito dónde se almacenan las conversaciones y las copias de seguridad.

☐ Consta por escrito dónde se ejecuta el modelo que las lee. Es una pregunta distinta de la anterior.

☐ Si algún tratamiento sale del Espacio Económico Europeo, está amparado por una decisión de adecuación o por garantías adecuadas, y documentado.

☐ El contrato obliga al proveedor a avisar antes de cambiar la ubicación.

05 Entrenamiento con las conversaciones

☐ El proveedor del agente confirma por escrito si usa las conversaciones para entrenar modelos.

- [ ] El proveedor del modelo de lenguaje lo confirma por escrito también. Que uno no entrene no cubre al otro.
- [ ] La respuesta está en el contrato y no solo en una página informativa.
- [ ] Si hubiera algún uso para mejorar el servicio, consta cuál, con qué datos y cómo se desactiva.

06 Subencargados

- [ ] El proveedor entrega la lista vigente de subencargados, con finalidad y ubicación de cada uno.
- [ ] El proveedor del modelo de lenguaje figura en la lista.
- [ ] El contrato fija cuánto antes se avisa de un alta o una sustitución y qué puede hacer la empresa si se opone.
- [ ] Cada subencargado queda sujeto a obligaciones de protección de datos equivalentes a las del contrato.

07 Conservación y borrado

- [ ] La empresa puede fijar cuánto tiempo se conservan las conversaciones, o sabe cuánto las conserva el proveedor.
- [ ] Consta qué se borra al terminar el contrato, incluidas las copias de seguridad, y en cuánto tiempo.
- [ ] Hay un plazo para exportar los datos antes del borrado.
- [ ] Los registros técnicos del proveedor tienen una retención acotada.

08 Derechos de las personas

- [ ] Se pueden localizar todas las conversaciones y los datos asociados a una persona concreta.
- [ ] Se pueden exportar, para atender el acceso y la portabilidad.
- [ ] Se pueden eliminar, y se sabe si eso alcanza a las copias.
- [ ] El proveedor redirige a la empresa las solicitudes que reciba de las personas y se lo comunica sin dilación.
- [ ] El procedimiento interno cabe en el plazo de un mes que fija el RGPD, prorrogable en los casos que la norma prevé.

09 Decisiones automatizadas

- [ ] Están identificadas las decisiones que el agente podría tomar y que afectan de forma significativa a un cliente, como denegar un reembolso, dar de baja o limitar un servicio.
- [ ] Para esas decisiones hay una persona en medio, o una base jurídica y unas garantías documentadas.
- [ ] El agente resuelve lo que favorece o informa al cliente, y pasa a una persona lo que puede perjudicarle.
- [ ] Se puede consultar qué sesiones ha ejecutado el agente, cuándo y con qué resultado.

10 Brechas, evaluación de impacto y registro

☐ El contrato obliga al proveedor a comunicar sin dilación indebida las brechas, y fija un plazo máximo.

☐ La empresa sabe quién decide si hay que notificar a la autoridad de control, que es quien responde ante ella.

☐ El delegado de protección de datos, o quien haga sus veces, ha valorado si hace falta una evaluación de impacto.

☐ El registro de actividades está actualizado con el agente.

11 Notas para datos de salud y para entidades financieras

☐ Si el agente puede recibir datos de salud, hay una circunstancia del artículo 9.2 del RGPD que levanta la prohibición, anotada por escrito. Un tratamiento a gran escala de estos datos exige evaluación de impacto.

☐ Si la empresa es una entidad financiera dentro del ámbito del Reglamento DORA, el contrato con el proveedor de servicios de TIC cumple sus cláusulas contractuales fundamentales, además de las del RGPD.

12 Registro de la reunión

Una fila por punto. Sin respuesta escrita y sin documento, el punto queda pendiente.

Punto	Respuesta del proveedor	Documento que lo prueba	Pendiente y responsable
Base jurídica y finalidades	☐	[Registro de actividades]	☐
Información a las personas y aviso de IA	☐	[Política de privacidad, primer mensaje]	☐
Contrato de encargado	☐	[Anexo de tratamiento de datos]	☐
Ubicación de datos y modelos	☐	[Contrato y lista de subencargados]	☐
Entrenamiento	☐	[Contrato, del proveedor y del modelo]	☐
Subencargados	☐	[Lista vigente y procedimiento de cambio]	☐
Conservación y borrado	☐	[Política de conservación]	☐
Derechos de las personas	☐	[Procedimiento interno]	☐
Decisiones automatizadas	☐	[Reglas del agente y de escalado]	☐
Brechas de seguridad	☐	[Contrato y plan de respuesta]	☐

13

Decisión

Resultado de la reunión [se puede activar / se activa con condiciones / no se activa todavía]. Condiciones y pendientes [lista]. Responsable de cada pendiente y fecha [nombres y fechas]. Próxima revisión [fecha, por ejemplo cuando cambie un subencargado o un canal].