Lista de comprobación para un agente de IA de soporte con datos de salud

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]

PRODUCTO
[Nombre del producto]

REUNIÓN
[fecha]

ASISTEN
[soporte, legal y protección de datos]

LA LISTA, EN CIFRAS

9	2	Art. 9	Art. 35
Apartados con casillas	Cuadros para rellenar	Categoría especial del RGPD	Evaluación de impacto

00 Datos de la reunión

Empresa [Nombre de la empresa]. Producto [Nombre del producto]. 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]. Asisten por legal, por protección de datos, por soporte y por producto [nombres].

A quién atiende el soporte [centros, clínicas, profesionales]. Quién escribe [personal de administración, profesionales sanitarios, responsables de sistemas]. Si el soporte atiende también a pacientes, se anota aquí, porque cambia el apartado 4.

01 Qué papel tiene la empresa con cada dato

- ☐ Están separados por escrito los dos grupos de datos que toca el soporte. Los de las personas que usan el producto en cada centro, como nombre, correo, centro, plan y facturas. Y los de pacientes, que viven dentro del producto.
- ☐ Para los datos de las personas que usan el producto consta quién es responsable del tratamiento.
- ☐ Para los datos de pacientes consta si la empresa actúa como encargada del tratamiento por cuenta de cada centro, y en qué contrato.
- ☐ El contrato con cada centro dice si el soporte puede acceder a datos de pacientes, para qué y con qué límites.
- ☐ El registro de actividades de tratamiento recoge la atención al cliente con un agente de IA.

02 Qué puede ver el agente y qué no

Una fila por tipo de dato. La respuesta por defecto para los datos de pacientes es no. Si alguna fila necesita un sí, el motivo se escribe y lo firma quien decide.

Dato	¿Lo ve el agente?	Para qué	Quién lo decide
Nombre, correo y centro de quien escribe	[sí / no]	[Identificar la cuenta]	[Nombre]
Plan contratado, usuarios y estado de la facturación	[sí / no]	[Motivo]	[Nombre]
Documentación y artículos de ayuda del producto	[sí / no]	[Responder]	[Nombre]
Configuración del centro, como agendas, profesionales y permisos	[sí / no]	[Motivo]	[Nombre]
Datos de pacientes, como nombre, citas, historia clínica e informes	[no]	[No hacen falta para una duda de uso]	[Nombre]
Capturas de pantalla y adjuntos que envía el usuario	[sí / no]	[Pueden mostrar datos de pacientes]	[Nombre]
Registros técnicos del producto	[sí / no]	[Motivo]	[Nombre]

03 Minimización

- ☐ Cada sí del cuadro anterior tiene un motivo escrito. Lo que no hace falta para atender no llega al agente, como pide el artículo 5.1.c del RGPD.
- ☐ Las acciones con las que el agente consulta los sistemas de la empresa devuelven solo los campos necesarios, y ninguna devuelve datos de pacientes.
- ☐ La documentación y los ejemplos con los que responde el agente no contienen datos de pacientes, tampoco en las capturas de pantalla.

- [ ] El chat y el formulario de soporte no piden datos clínicos y avisan de que no se escriban.
- [ ] Consta cuánto tiempo se conservan las conversaciones y los adjuntos, y quién puede acortarlo.

04 Categoría especial del artículo 9 y su base

- [ ] Legal ha decidido por escrito si el soporte trata datos de salud de forma prevista, o solo de forma accidental cuando un usuario los envía.
- [ ] Si el tratamiento está previsto, consta qué circunstancia del artículo 9.2 del RGPD levanta la prohibición, además de la base jurídica del artículo 6.
- [ ] Si esa circunstancia es la de las letras g), h) o i), consta la norma con rango de ley que la ampara, como pide el artículo 9.2 de la Ley Orgánica 3/2018.
- [ ] Si la empresa actúa como encargada, las instrucciones documentadas del centro cubren este uso.
- [ ] Si el tratamiento no está previsto, están escritos el aviso al usuario y el procedimiento del apartado 9.

05 Evaluación de impacto y delegado de protección de datos

- [ ] El delegado de protección de datos, o quien haga sus veces, ha valorado por escrito si hace falta una evaluación de impacto antes de activar el agente.
- [ ] La valoración tiene en cuenta el artículo 35.3.b del RGPD, que la exige para el tratamiento a gran escala de categorías especiales.
- [ ] La valoración se ha contrastado con la lista de la AEPD. Según ella, la evaluación es necesaria en la mayoría de los casos que cumplen dos o más criterios, entre ellos el uso de categorías especiales, el uso de datos a gran escala y el uso de nuevas tecnologías.
- [ ] Si la evaluación corresponde al centro como responsable, la empresa le facilita la información que necesita para hacerla.
- [ ] Consta si la empresa está obligada a designar delegado por el artículo 37.1.c del RGPD, y quién es.

06 Encargado y subencargados

- [ ] Hay un contrato de encargado firmado con el proveedor del agente de IA, con el contenido del artículo 28.3 del RGPD.
- [ ] Si la empresa es encargada de los centros y el agente puede recibir datos de pacientes, el proveedor del agente es otro encargado. Consta la autorización previa y por escrito de cada centro, específica o general, que exige el artículo 28.2.
- [ ] Si la autorización es general, los centros han sido informados del alta del proveedor y han tenido ocasión de oponerse.
- [ ] El proveedor del agente asume las mismas obligaciones de protección de datos que la empresa tiene con los centros, como exige el artículo 28.4.
- [ ] El proveedor del modelo de lenguaje figura en la lista de subencargados del proveedor del agente.

07 Dónde se procesan los datos

- ☐ Consta por escrito dónde se almacenan las conversaciones, los adjuntos y las copias de seguridad.
- ☐ Consta por escrito dónde se ejecuta el modelo de lenguaje que las lee.
- ☐ Consta por escrito que ni el proveedor del agente ni el del modelo entrenan modelos con las conversaciones.
- ☐ Si algún tratamiento sale del Espacio Económico Europeo, está amparado y documentado.

08 Seguridad y registro de accesos

- ☐ Solo ven las conversaciones las personas que las necesitan, con cuentas personales y roles.
- ☐ Queda registro de qué acciones ejecuta el agente sobre los sistemas de la empresa, con su fecha y su resultado.
- ☐ Consta qué registro de accesos a las conversaciones ofrece el proveedor y durante cuánto tiempo se conserva.
- ☐ Las medidas de seguridad son adecuadas al riesgo, como pide el artículo 32 del RGPD, con cifrado en tránsito y en reposo y capacidad de restaurar los datos.
- ☐ El personal del proveedor con acceso a las conversaciones es el mínimo y está sujeto a confidencialidad.
- ☐ El proveedor comunica las brechas sin dilación indebida. La empresa sabe quién avisa a cada centro y quién notifica a la autoridad de control, en un máximo de 72 horas cuando la notificación procede.

09 Si un usuario pega datos clínicos en el chat

- ☐ El agente no repite, no resume y no usa los datos clínicos en su respuesta.
- ☐ El agente contesta con el mensaje previsto y pasa la conversación a una persona del equipo.
- ☐ La persona resuelve la duda sin copiar los datos a otros sistemas, como notas internas, tareas, correo o el canal del equipo.
- ☐ Está decidido qué se hace con el mensaje y con el adjunto. Si se eliminan, quién lo hace, en qué plazo y si alcanza a las copias.
- ☐ Está decidido cuándo se avisa al delegado de protección de datos y cuándo al centro.
- ☐ Cada caso se anota en un registro, sin los datos clínicos, para ver si se repite y corregir la causa.

10 Instrucciones para el agente

- ☐ El agente tiene escrito que no pide datos de pacientes ni información clínica.
- ☐ Tiene escrito qué hace cuando los recibe, con las palabras del apartado 9.
- ☐ Tiene escrito que no da consejo médico ni interpreta información clínica.

- [ ] Las instrucciones se han probado antes de publicarlas, con mensajes y capturas de ejemplo que simulan datos clínicos.
- [ ] Una persona revisa una muestra de conversaciones cada [periodicidad].

11 Registro de la reunión

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

Punto	Respuesta	Documento que lo prueba	Pendiente y responsable
Papel de la empresa con cada dato	☐	[Contratos con los centros]	☐
Qué ve el agente y qué no	☐	[Cuadro del apartado 2]	☐
Minimización	☐	[Configuración del agente y de sus acciones]	☐
Categoría especial y su base	☐	[Nota de legal]	☐
Evaluación de impacto	☐	[Valoración del delegado]	☐
Encargado y subencargados	☐	[Contrato y autorización de los centros]	☐
Dónde se procesan los datos	☐	[Contrato y lista de subencargados]	☐
Seguridad y registro de accesos	☐	[Medidas y registros]	☐
Datos clínicos en el chat	☐	[Procedimiento escrito]	☐
Instrucciones del agente	☐	[Texto de las instrucciones y pruebas]	☐

12 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, o cuando cambie un canal, una acción del agente o un subencargado].