

MEDAI · TOOLDATA SPA

Contrato de encargo del tratamiento (DPA)

Modelo conforme a la Ley 21.719 — tratamiento de datos sensibles de salud

Activo de confianza · MedAI en pre-lanzamiento · julio de 2026

Modelo conforme a la Ley N° 21.719 (Chile)

⚠ DOCUMENTO MODELO — NO ES ASESORÍA LEGAL. Esta plantilla es un punto de partida para el contrato de encargo del tratamiento entre una institución de salud (Responsable) y Tooldata SpA (Encargado) en el contexto del producto MedAI. **Debe ser revisada y adaptada por un abogado habilitado en Chile** antes de su uso o firma, y ajustada al texto vigente de la Ley N° 21.719, su reglamento y las instrucciones de la Agencia de Protección de Datos Personales. Los campos entre corchetes [...] deben completarse. Las referencias a plazos (p. ej. 72 horas) y artículos deben verificarse con el texto legal vigente.

Comparecientes

En [ciudad], a [fecha], entre:

- **El Responsable:** [Razón social de la institución de salud], RUT [•], domicilio en [•], representada por [•] (en adelante, el «**Responsable**»); y
- **El Encargado: Tooldata SpA**, RUT 76.963.629-3, domicilio en Avenida Concón Reñaca 4000, oficina 1603, Concón, Región de Valparaíso, representada por [•] (en adelante, el «**Encargado**»).

En conjunto, las «Partes». Este Acuerdo de Tratamiento de Datos (el «**DPA**») forma parte integrante y es anexo del Contrato de Prestación de Servicios suscrito entre las Partes para la provisión del software **MedAI** (el «Contrato Principal»). En caso de contradicción en materia de protección de datos, prevalece este DPA.

1. Marco y objeto

1.1. El presente DPA regula el tratamiento de datos personales que el Encargado realice **por cuenta y según las instrucciones del Responsable** con ocasión de la prestación del servicio MedAI, conforme a la **Ley N° 21.719** sobre protección de datos personales y demás normativa aplicable.

1.2. Las Partes reconocen que el Responsable determina los fines y medios del tratamiento y que el Encargado actúa exclusivamente en calidad de **encargado de tratamiento**.

1.3. Para los despliegues **on-premise** o en **nube privada (VPC)** del Responsable, los datos clínicos residen en la infraestructura controlada por el Responsable. El acceso del Encargado se limita a las actividades de soporte, mantenimiento y actualización expresamente autorizadas en el Anexo I y en las instrucciones del Responsable.

2. Definiciones

Para los efectos de este DPA, los términos «dato personal», «dato personal sensible», «tratamiento», «responsable», «encargado», «titular», «vulneración de datos», «evaluación de impacto» y «Agencia» tendrán el significado que les asigna la Ley N° 21.719. Se deja constancia de que los **datos de salud constituyen datos personales sensibles** sujetos a régimen reforzado.

3. Instrucciones del Responsable

3.1. El Encargado tratará los datos **únicamente conforme a las instrucciones documentadas** del Responsable, incluidas las relativas a transferencias internacionales, salvo obligación legal que lo requiera (en cuyo caso informará al Responsable, salvo prohibición legal).

3.2. El Encargado informará al Responsable si, a su juicio, una instrucción infringe la Ley N° 21.719 u otra normativa de protección de datos.

3.3. El alcance, naturaleza y finalidad del tratamiento, los tipos de datos y las categorías de titulares se describen en el **Anexo I**.

4. Confidencialidad

4.1. El Encargado garantiza que las personas autorizadas para tratar los datos se han comprometido a respetar la **confidencialidad** y el **secreto** (incluido, cuando corresponda, el secreto médico) o están sujetas a una obligación legal de confidencialidad.

4.2. El acceso a los datos se limita al personal que lo necesite para prestar el servicio (**necesidad de conocer**), bajo control de acceso por rol.

5. Medidas de seguridad

5.1. El Encargado implementará y mantendrá las **medidas técnicas y organizativas** apropiadas para garantizar un nivel de seguridad adecuado al riesgo, descritas en el **Anexo II**, incluyendo cifrado en tránsito y en reposo, control de acceso, registros de auditoría y trazabilidad.

5.2. El Encargado no utilizará los datos del Responsable para entrenar modelos de inteligencia artificial de uso general o de terceros, ni los compartirá con terceros fuera de lo previsto en este DPA.

6. Subencargados (subprocesadores)

6.1. El Responsable **autoriza** el uso de los subencargados listados en el **Anexo III**.

6.2. El Encargado informará al Responsable de cualquier incorporación o sustitución de subencargados con una antelación razonable, permitiéndole **oponerse** por motivos fundados de protección de datos.

6.3. El Encargado impondrá a cada subencargado, mediante contrato, **obligaciones de protección de datos equivalentes** a las de este DPA, y responderá ante el Responsable por el incumplimiento de sus subencargados.

7. Asistencia al Responsable

7.1. **Derechos de los titulares.** El Encargado asistirá al Responsable, mediante medidas técnicas y organizativas apropiadas, para atender las solicitudes de ejercicio de derechos (acceso, rectificación, cancelación o supresión, oposición, portabilidad y bloqueo). Si un titular se dirige al Encargado, este lo derivará al Responsable sin responder directamente, salvo instrucción en contrario.

7.2. **EIPD y consultas.** El Encargado asistirá al Responsable en la realización de **evaluaciones de impacto en protección de datos (EIPD)** y, cuando corresponda, en las consultas previas a la Agencia, proporcionando la información de su ámbito (ver plantilla EIPD de MedAI).

8. Notificación de vulneraciones (brechas)

8.1. El Encargado notificará al Responsable **sin dilación indebida** tras tener conocimiento de una **vulneración de la seguridad** que afecte datos personales tratados por cuenta del Responsable, a fin de que este pueda cumplir su deber de notificación a la **Agencia** y, cuando proceda, a los titulares, dentro de los plazos legales (referencialmente, **72 horas** — a confirmar con la norma vigente).

8.2. La notificación incluirá, en la medida disponible: naturaleza de la vulneración, categorías y volumen aproximado de datos y titulares afectados, consecuencias probables y medidas adoptadas o propuestas.

9. Transferencias internacionales

9.1. El Encargado no transferirá datos fuera de Chile sin instrucción o autorización del Responsable y sin garantías adecuadas conforme a la Ley N° 21.719.

9.2. Las Partes reconocen que el subencargado de correo transaccional (notificaciones del formulario del sitio web) almacena datos en **Estados Unidos**; dicha transferencia se rige por el contrato y las garantías indicadas en el **Anexo III**. En los despliegues on-premise/VPC del producto, los datos clínicos **no se transfieren** fuera de la infraestructura del Responsable.

10. Devolución o destrucción

Al término de la prestación, y a elección del Responsable, el Encargado **devolverá o destruirá** todos los datos personales tratados por cuenta del Responsable y suprimirá las copias existentes, salvo obligación legal de conservación, **certificando** por escrito dicha devolución o destrucción.

11. Registro y auditoría

11.1. El Encargado mantendrá un **registro de las actividades de tratamiento** efectuadas por cuenta del Responsable.

11.2. El Encargado pondrá a disposición del Responsable la información necesaria para demostrar el cumplimiento de este DPA y permitirá y contribuirá a **auditorías**, incluidas inspecciones, realizadas por el Responsable o un auditor mandatado, con preaviso razonable y bajo confidencialidad.

12. Obligaciones del Responsable

El Responsable garantiza que cuenta con una **base de legitimación** válida para el tratamiento (incluido el régimen de datos sensibles de salud), que sus instrucciones son lícitas y que ha cumplido sus deberes de información hacia los titulares.

13. Responsabilidad

Cada Parte responderá conforme a la Ley N° 21.719 y al Contrato Principal. [Cláusula de responsabilidad e indemnidad — a definir por las Partes y revisar legalmente.]

14. Vigencia y terminación

Este DPA estará vigente mientras el Encargado trate datos por cuenta del Responsable, y subsistirán las obligaciones que por su naturaleza deban perdurar (confidencialidad, devolución/destrucción).

Anexo I — Descripción del tratamiento

- **Roles:** Responsable = [institución de salud]; Encargado = Tooldata SpA.
- **Objeto:** apoyo a la documentación y al lenguaje clínico, y/o a la imagenología, mediante MedAI, con validación humana (human-in-the-loop).
- **Naturaleza y finalidad:** generación de borradores (epicrisis, resúmenes, informes), propuestas de codificación CIE-10 y apoyo a la decisión clínica, sujetos a revisión y firma de un profesional habilitado. MedAI no emite diagnóstico autónomo.
- **Categorías de titulares:** pacientes; profesionales de salud y usuarios del Responsable.
- **Categorías de datos:** datos de identificación; **datos de salud (sensibles)**; según módulo, imágenes médicas (DICOM); metadatos de uso y registros de auditoría.
- **Duración:** la del Contrato Principal, salvo término anticipado.

Anexo II — Medidas de seguridad (referenciales; completar según despliegue)

- Cifrado en tránsito (TLS) y en reposo (AES).
- Control de acceso por rol e inicio de sesión único (SAML/OIDC).
- Registros de auditoría, trazabilidad y versionado de las salidas.
- Segregación de datos; retención configurable y mecanismos de enmascaramiento/anonimización.
- Despliegue on-premise / VPC: los datos clínicos no salen de la infraestructura del Responsable; capacidad de operación air-gapped.

- Gestión de actualizaciones controladas y versionadas; respaldos y plan de recuperación.
- Política de **no uso** de datos del cliente para entrenar modelos de uso general.

Anexo III – Subencargados autorizados (completar)

Subencargado	Servicio	Ubicación de datos	Garantías
Resend	Correo transaccional (notificaciones del formulario del sitio web; no datos clínicos del producto)	EE.UU.	Contrato de tratamiento de datos del proveedor
[Proveedor de hosting/VPS]	Infraestructura del sitio y microservicio de leads	[Chile / •]	[Contrato / medidas]
[Otros]	[•]	[•]	[•]

Firmas: Responsable [•] — Encargado: Tooldata SpA [•]. *Última actualización del modelo: junio de 2026. Sujeto a revisión legal.*