SEGURTASUN-DOSIERRA

# Zure datuen segurtasuna eta konfidentzialtasuna

*Zure betetze-arduradunak bulegoak bezeroen dokumentuak igotzen uzteko behar duena.*

| HONENTZAT | DATA | BERTSIOA | ARDURADUNA |
|---|---|---|---|
| Bulegoak eta aholkularitzak | 26/11/2026 | 1.226.12 | Biomag S.L.U. |

## Funtsezkoa

| | |
|---|---|
| Tus datos no entrenan modelos | Las consultas y los documentos se usan solo para responderte; nunca para entrenar modelos ni para terceros. |
| Datos personales fuera del modelo, por defecto | Nombres, DNI, NIE, NIF, cuentas, correos y teléfonos viajan al modelo como marcadores y vuelven a su sitio en tu pantalla. El modelo trabaja el caso sin ver a las personas. |
| Retención cero con los modelos | Los modelos de lenguaje se invocan con la opción de no retención de datos donde el proveedor la ofrece, como fija el contrato de encargado. |
| Alojado en la UE (Ámsterdam) | La aplicación, la caché, la base de datos y los documentos se guardan en centros de datos de la Unión Europea, en los Países Bajos. |
| Cada despacho, su espacio | Ninguna organización ve los datos de otra; se comprueba en cada despliegue y, si falla, no se despliega. |
| Contrato de encargado firmado en línea | El contrato del art. 28 RGPD se firma desde tu cuenta, con su versión y su huella, y descargas la copia. |
| Lo que no hace falta se borra solo | Los registros se purgan al cumplir el plazo de conservación, sin que lo pidas; puedes exportar o suprimir tus datos cuando quieras. |

## Gaur, neurtuta

| | |
|---|---|
| Erregistroen kontserbazio-epea | 365 egun |
| Azken garbiketa automatikoa | 26/11/2026 02:48 |
| Erakundeen arteko isolamendu-egiaztapenak | 22 |

## Segurtasun-kontrolak: ISO/IEC 27001 eta ENS arauen araberako autoebaluazioa, eta nola egiaztatu

| KONTROLA | NEURRIA | NOLA EGIAZTATZEN DEN |
|---|---|---|
| Control de acceso y restricción de la información (ISO 5.15 · 8.3 · ENS op.acc) | Cada organización ve solo lo suyo: toda consulta a la base filtra por organización, y el acceso es por persona y por rol, con sesiones que se revocan. | Las comprobaciones de aislamiento corren en cada despliegue; si una falla, no se despliega. |
| Autenticación segura (ISO 8.5 · ENS op.acc) | PIN guardado con bcrypt, enlace de un solo uso por correo y bloqueo tras intentos fallidos. | Cinco PIN erróneos seguidos bloquean la cuenta durante unos minutos. |
| Uso de criptografía (ISO 8.24 · ENS mp.com · mp.info) | Todo el tráfico va cifrado y el navegador lo exige (HSTS); el contenido de los expedientes se guarda cifrado en la base de datos. | curl -sI https://www.aim-lex.ai \| grep -i strict-transport |
| Eliminación de la información (ISO 8.10 · ENS mp.info) | Lo que deja de ser necesario se borra solo, sin que lo pidas, al cumplir el plazo de conservación. | La fecha de la última limpieza se publica en la página de Seguridad (www.aim-lex.ai/seguridad). |
| Prevención de fugas de datos (ISO 8.12 · ENS mp.info) | El texto que se comprueba en el verificador público no se guarda: solo su huella SHA-256. | Comprueba dos veces el mismo texto: el sello da la misma huella y el texto no aparece. |
| Privacidad y protección de datos personales (ISO 5.34 · ENS mp.info) | Contrato de encargado del tratamiento (art. 28 RGPD) con la lista de subencargados; la aplicación y la base de datos, alojadas en la Unión Europea. | El contrato y la lista, publicados. |
| Servicios externos y en la nube (ISO 5.23 · ENS op.ext · op.nub) | Cada proveedor que interviene, con su función, su ubicación y la garantía para las transferencias. | La tabla de subencargados. |
| Gestión de vulnerabilidades técnicas (ISO 8.8 · ENS op.exp) | Cada noche se buscan secretos en todo el historial del código, se analiza el código con reglas de seguridad, se revisan las dependencias contra OSV y el catálogo de vulnerabilidades explotadas de la CISA (con su probabilidad de explotación), se genera la lista de materiales del software (SBOM) y se hace un escaneo pasivo de la web con OWASP ZAP. | Los pasos del flujo de integración continua: secretos, «Dependencias contra vulnerabilidades conocidas», lista de materiales y escaneo de la web. |
| Desarrollo seguro y pruebas de seguridad (ISO 8.28 · 8.29 · ENS mp.sw) | Regresión de seguridad y la batería completa antes de cada despliegue; una vez por versión, ataques simulados contra el propio servicio (fuga de instrucciones, normas inventadas, órdenes escondidas en documentos); la política de contenido solo deja ejecutar código de este dominio. | curl -sI https://www.aim-lex.ai \| grep -i content-security-policy |

| KONTROLA | NEURRIA | NOLA EGIAZTATZEN DEN |
|---|---|---|
| Registro y seguimiento (ISO 8.15 · 8.16 · ENS op.exp · op.mon) | Los errores quedan registrados con su contexto, y cada noche un vigilante recorre el servicio y da la alarma si algo falla. | El estado del sistema es público. |

## Tratamendu-arduradunaren kontratutik: betebeharrak, neurriak eta azpikontratatuak

### 3. Obligaciones de AIM LEX como encargado

- **Solo por instrucción del Cliente.** No tratamos los datos para ninguna finalidad propia. **No entrenamos modelos con el contenido del Cliente**, ni cedemos sus datos a terceros con ese fin.
- **Confidencialidad.** Quien accede a los sistemas está sujeto a deber de secreto, que subsiste tras el fin de la relación.
- **Aislamiento entre clientes.** Cada organización solo accede a sus propios datos. Es una regla del código verificada por pruebas automáticas en cada despliegue, no una configuración que alguien pueda olvidar.
- **Ayuda con los derechos de los interesados.** El Cliente puede exportar todos sus datos en cualquier momento desde la propia aplicación, y solicitar la supresión de un usuario y de su rastro.
- **Notificación de brechas.** Comunicaremos al Cliente cualquier violación de seguridad que afecte a sus datos sin dilación indebida desde que tengamos constancia, con la información necesaria para que cumpla su obligación de notificar.
- **Devolución o supresión al terminar.** A elección del Cliente, le devolvemos sus datos o los suprimimos al finalizar la prestación, salvo obligación legal de conservación.
- **Puesta a disposición de información.** Facilitamos al Cliente lo necesario para demostrar el cumplimiento y para permitir auditorías.

### 4. Medidas de seguridad (artículo 32)

Estas son las que aplicamos hoy:

- **Cifrado en tránsito** en todas las comunicaciones, y en reposo en la infraestructura de base de datos.
- **Retención limitada y purga automática.** Los registros de consulta se purgan automáticamente pasada la ventana de retención configurada (365 días por defecto). Un proceso diario los elimina sin intervención humana.
- **El texto verificado no se conserva.** Cuando el Cliente comprueba las citas de un escrito, guardamos su huella SHA-256 y el resultado, **no el texto**. La huella permite acreditar a qué documento corresponde la comprobación sin custodiar el documento.
- **Subencargados con retención cero.** Los modelos de lenguaje se invocan con la opción de no retención de datos (zero data retention) donde el proveedor la ofrece; cuando no está disponible para un modelo, se enruta a un proveedor que sí la garantiza.

- **Seudonimización antes del modelo, activada por defecto.** Los nombres de las personas, los DNI, NIE y NIF, las cuentas IBAN, los correos y los teléfonos se sustituyen por marcadores antes de enviar el texto al modelo y se restituyen en la respuesta. La tabla de equivalencias solo existe en memoria mientras dura cada tarea. El Cliente puede desactivarla en «Tu cuenta».
- **Control de acceso** por organización y por rol, con sesiones caducables.
- **Registro de operaciones** sobre los datos, para poder reconstruir qué ocurrió.

### 5. Subencargados

El Cliente autoriza a los siguientes subencargados, cuya función es exclusivamente técnica:

- Railway · Alojamiento en los Países Bajos (región europe-west4) de la aplicación, la caché y la base de datos, y almacén de archivos en Ámsterdam · UE (Países Bajos) · empresa de EE. UU.
- Anthropic · Modelos de lenguaje (generación y verificación) · EE. UU. · cláusulas contractuales tipo
- OpenRouter · Enrutado a modelos con retención cero · EE. UU. · cláusulas contractuales tipo
- Resend · Envío de correo transaccional · UE · EE. UU.
- Mistral AI · Modelos de lenguaje de la opción «Modelo europeo» y transcripción de grabaciones · UE (Francia)

Informaremos al Cliente de cualquier cambio previsto en esta lista, dándole la oportunidad de oponerse.

### 6. Transferencias internacionales

Las transferencias fuera del Espacio Económico Europeo se amparan en cláusulas contractuales tipo aprobadas por la Comisión Europea, con las medidas complementarias aplicables.

Kontratu osoa www.aim-lex.ai/encargado helbidean dago eta zure kontutik sinatzen da lineaz. Segurtasun-zalantzak edo zure bulegoaren berrikuspena: idatzi iezaguzu www.aim-lex.ai/contacto helbidetik. Kontratuaren bertsioa: 08/11/2026.