MARKETDRONES

Política de privacidad

Versión del 8 de noviembre de 2026

1. Responsable del tratamiento y contacto

1. El responsable del tratamiento de los datos personales en relación con MarketDrones es SentioLab sp. z o.o., con domicilio social en Nowy Kiełbów 32, 26-806 Stara Błotnica, Polonia, inscrita en el registro polaco con KRS 0000495860, NIP 7010410720 y REGON 147082076 (el «Responsable»). Dirección de correspondencia: ul. Nowoursynowska 161 L, 02-787 Varsovia, Polonia.
2. Para consultas y solicitudes sobre privacidad: info@marketdrones.net. Sitio web: https://marketdrones.net/.
3. Esta Política se aplica a los datos relacionados con las visitas al sitio web, el registro y las cuentas, las funciones de los Usuarios en la Organización, el seguimiento de fuentes públicas, los estudios encargados y las grabaciones de procesos de solicitud, la facturación, la seguridad y las comunicaciones. Una Organización puede ser responsable independiente del tratamiento de los datos que gestione para sus propias finalidades fuera del Servicio.

2. Personas interesadas y categorías de datos

Personas interesadas	Categorías de datos
Usuarios, Administradores y personas invitadas	Dirección de correo, nombre o identificador, Organización, función y permisos, estado de la cuenta y Suscripción, invitaciones, ajustes de informes y alertas, marcas vigiladas, solicitudes de investigación, aceptación de documentos y preferencias comerciales.
Representantes y personas de contacto de Organizaciones	Datos profesionales de contacto, correspondencia, solicitudes de asistencia y datos necesarios para gestionar el contrato.
Personas vinculadas a la facturación	Datos de empresa y factura, contacto de facturación, registros de pagos y liquidaciones y su estado. No recogemos números completos de tarjeta ni códigos CVV.
Visitantes del sitio y Usuarios del Panel	Dirección IP, identificadores de sesión, datos del navegador y dispositivo necesarios para el funcionamiento, información de errores y sucesos técnicos o de seguridad.

Personas interesadas	Categorías de datos
Personas que aparecen en materiales de fuentes vigiladas	Datos personales incidentales presentes en páginas o documentos públicos, como nombres, cargos profesionales, contactos o firmas; el Servicio no pretende vigilar a personas particulares.
Participantes en investigaciones de procesos de solicitud	Interacciones con formularios, tipo de dispositivo, semana del estudio, género y franja de edad del participante, si se recibieron ofertas y los datos que puedan aparecer en las grabaciones de trabajo. Antes de compartir una grabación se minimizan u ocultan identificadores innecesarios, credenciales e información confidencial.
Personas vinculadas a abusos confirmados del acceso gratuito	Identificadores mínimos necesarios para detectar reincidencias, fecha de confirmación, motivo del bloqueo y, en su caso, nota breve de la revisión.

No realizamos seguimiento comercial del comportamiento ni guardamos un historial de los materiales analíticos que consultan los Usuarios o de sus búsquedas. Solo mantenemos los registros técnicos necesarios para la seguridad y las operaciones administrativas esenciales descritas a continuación.

3. Finalidades y bases jurídicas del tratamiento

Finalidad	Base jurídica conforme al RGPD
Registro, autenticación, cuentas, permisos y prestación B2B	Art. 6.1.f del RGPD: interés legítimo en ejecutar el contrato con la Organización y atender a sus representantes; puede aplicarse también el art. 6.1.b cuando el interesado sea parte del contrato.
Invitaciones, administración de Organizaciones y operaciones administrativas	Art. 6.1.f: gestión adecuada y responsabilidad de las operaciones.
Facturación, contabilidad e impuestos	Art. 6.1.c: obligaciones legales; en su caso, art. 6.1.b o f para ejecutar el contrato.
Informes semanales, alertas y avisos de cuenta, seguridad y facturación	Art. 6.1.f: prestación del Servicio a la Organización; o art. 6.1.b si el interesado es parte contractual.
Contacto, asistencia y reclamaciones	Art. 6.1.b o f; art. 6.1.c cuando exista una obligación legal concreta.

Finalidad	Base jurídica conforme al RGPD
Funcionamiento técnico, seguridad, incidentes y prevención de abusos del acceso gratuito	Art. 6.1.f: seguridad y prevención de fraude y elusión de condiciones, sujeto a evaluación documentada de necesidad y ponderación.
Correo comercial voluntario de MarketDrones y SentioLab	Art. 6.1.a: consentimiento, junto con las exigencias aplicables de la Ley polaca de comunicaciones electrónicas.
Recopilación y presentación de análisis de cambios en sitios y documentos públicos	Art. 6.1.f: interés legítimo en documentar y analizar cambios del mercado, sujeto a proporcionalidad y minimización de datos personales.
Realización de investigaciones de competencia encargadas y acceso a grabaciones de solicitudes	Art. 6.1.f: interés legítimo en investigar el mercado y prestar el Servicio a la Organización, sujeto a evaluación de necesidad y ponderación; se utiliza otra base adecuada cuando sea legalmente exigible.
Formulación, ejercicio y defensa de reclamaciones y cumplimiento de requerimientos legales	Art. 6.1.f o c, según corresponda.

El consentimiento para comunicaciones comerciales es independiente, voluntario y no está premarcado. Puede retirarse desde la configuración de la cuenta o mediante un enlace de cada mensaje pertinente; ello detendrá el envío de publicidad, sin afectar a la licitud del tratamiento anterior ni a las comunicaciones esenciales del Servicio.

4. Procedencia de los datos

Recibimos datos de los Usuarios y representantes de las Organizaciones; de sus Administradores (por ejemplo, al invitar a un miembro del equipo); de sucesos técnicos y de seguridad; de proveedores que intervienen en pagos; de sitios web y documentos de acceso público vigilados por MarketDrones; y, en los estudios de procesos de solicitud, de los participantes y de las interacciones realizadas en la investigación encargada. La disponibilidad pública de un material no suprime la protección de los datos personales ni permite su reutilización sin límites.

Respecto a las personas mencionadas en fuentes vigiladas, el Responsable evalúa las obligaciones de información del artículo 14 del RGPD, las excepciones aplicables y las formas de ejercer los derechos. Si los datos se obtienen directamente de un participante de la investigación, se aplican las obligaciones informativas del artículo 13 del RGPD. Esta Política y nuestra dirección de contacto ofrecen información sobre las prácticas de seguimiento e investigación.

5. Destinatarios y proveedores

1. Los datos de una cuenta son accesibles para los Usuarios y Administradores autorizados de la misma Organización según sus funciones. Un Administrador puede ver operaciones administrativas importantes, pero no el historial de accesos del personal, las direcciones IP ni sus búsquedas o consultas analíticas.
2. El personal autorizado de SentioLab solo accede a datos de una Organización cuando resulta justificado para asistencia, incidentes, seguridad, facturación u obligaciones legales. El acceso se limita a lo necesario y se registra.
3. Alojamiento principal: MikrUs, en infraestructura identificada por el Prestador como ubicada en Finlandia. Los datos pueden ser tratados también por proveedores de correo profesional y transaccional, servicios contables y de facturación, proveedores de almacenamiento y reproducción técnica de grabaciones, proveedores de enlaces de pago en línea (si se utiliza ese método) y prestadores de asistencia técnica. Las facturas pueden comunicarse a autoridades y sistemas públicos, incluido el sistema polaco KSeF, cuando la ley lo exija.
4. Proveedor de análisis mediante IA: API de pago de Google Gemini, ejecutada con un proyecto de Cloud Billing activo y sin una restricción de procesamiento exclusiva para el Espacio Económico Europeo (EEE). Enviamos materiales de fuentes vigiladas, no datos de cuentas, facturación o preferencias individuales de Usuarios. No enviamos grabaciones de procesos de solicitud ni datos identificativos de participantes a la IA. Cuando es posible, reducimos o eliminamos los datos personales presentes de forma incidental en los textos antes de enviarlos.
5. Según las condiciones de los servicios de pago, Google declara que no utiliza los prompts ni los resultados enviados para mejorar sus productos o modelos de IA. Google describe la conservación de prompts, contexto y respuestas durante 55 días para seguridad y prevención de abusos. Las condiciones y documentos pueden actualizarse: https://ai.google.dev/gemini-api/terms y https://ai.google.dev/gemini-api/docs/usage-policies.
6. Solo comunicamos datos a autoridades públicas cuando exista una base jurídica adecuada. No vendemos datos de Usuarios a anunciantes.

6. Transferencias internacionales

El tratamiento mediante la API Gemini puede tener lugar fuera del Espacio Económico Europeo, en países donde Google o sus subencargados dispongan de infraestructura. Solo afecta a los materiales realmente transmitidos a la API, que pueden contener incidentalmente datos personales procedentes de fuentes vigiladas.

Cuando se transfieren datos personales internacionalmente, el Responsable utiliza un mecanismo adecuado conforme al capítulo V del RGPD, como una decisión de adecuación o cláusulas contractuales tipo acompañadas de las garantías necesarias. La información sobre estas garantías puede solicitarse a través de nuestra dirección de contacto.

7. Plazos de conservación

Datos	Criterio de conservación
Cuentas activas de Usuarios, Organización y configuración	Durante el uso del Servicio; tras finalizar la Suscripción, 90 días de acceso limitado y después supresión, salvo excepción legal.
Solicitud de supresión de cuenta	Supresión de los sistemas activos tras una solicitud válida, salvo registros exigidos por ley o excepción antifraude justificada.
Copias de seguridad	Rotación y eliminación o sobrescritura automáticas en un máximo de 7 días; las restauraciones respetan supresiones anteriores.
Registros técnicos, de seguridad y accesos administrativos de SentioLab	Normalmente 180 días; más tiempo solo para incidentes, reclamaciones u obligaciones legales documentadas.
Historial de operaciones administrativas de la Organización	Normalmente 180 días; acceso limitado a los Administradores de dicha Organización.
Invitaciones a la Organización	Enlace válido durante 14 días; los datos de invitaciones no aceptadas, caducadas o canceladas se borran 30 días después de su caducidad o cancelación, salvo base legal adicional.
Historial de aceptación de Condiciones y consentimiento comercial	Hasta la supresión de la cuenta, salvo datos cuya conservación posterior sea legalmente obligatoria.
Reclamaciones	12 meses desde su resolución si la cuenta existe; tras una supresión válida de la cuenta, eliminación sin demora salvo obligación legal.
Facturas y documentación fiscal/contable	Solo durante el plazo exigido por la normativa tributaria y contable aplicable.
Abusos confirmados de acceso gratuito	12 meses desde la confirmación: identificadores mínimos, fecha y motivo del bloqueo; separados de cuentas eliminadas y solo cuando una evaluación de interés legítimo justifique conservarlos.

Datos	Criterio de conservación
Fuentes vigiladas con datos personales incidentales	Durante el tiempo justificado por el seguimiento histórico y el análisis de cambios.
Grabaciones de investigaciones encargadas y metadatos asociados	Durante el tiempo necesario para realizar el estudio, permitir el acceso a la Organización autorizada y, cuando sea necesario, proteger derechos. Se reducen o eliminan cuanto antes identificadores innecesarios. El acceso a reproducción termina con los permisos de Suscripción, sin perjuicio de la conservación técnica o legal necesaria.

7.1. Registro mínimo de abusos confirmados

1. El registro se utiliza exclusivamente para identificar intentos repetidos de eludir las condiciones de acceso gratuito, no para marketing, análisis de comportamiento ni perfiles comerciales.
2. La mera sospecha no basta para crear una anotación duradera. Una persona autorizada debe examinar las pruebas, confirmar el abuso y documentar una razón breve.
3. Solo se conservan los identificadores de Usuario u Organización realmente necesarios para detectar la repetición. El registro no incluye el perfil completo, el historial de navegación ni toda la correspondencia. Los identificadores seudonimizados o cifrados mediante hash también pueden constituir datos personales.
4. Las anotaciones se suprimen a los 12 meses de confirmar el abuso, salvo que otra obligación legal exija su conservación. El acceso se restringe al personal autorizado.
5. Una anotación puede conservarse después de la supresión de la cuenta únicamente si el Responsable ha documentado su base jurídica, necesidad y proporcionalidad. La persona interesada puede pedir reconsideración y ejercer el derecho de oposición y los demás derechos del RGPD.

8. Cookies, almacenamiento local y estadísticas anónimas

1. El sitio y el Panel utilizan exclusivamente cookies técnicas y/o almacenamiento local (localStorage) para inicio de sesión, sesiones, seguridad, funciones solicitadas por los Usuarios y preferencias de interfaz.
2. No utilizamos herramientas de seguimiento publicitario, píxeles de marketing, cookies analíticas no esenciales ni sistemas externos de análisis del comportamiento.
3. Bloquear los mecanismos de almacenamiento necesarios del navegador puede impedir el inicio de sesión o determinadas funciones.
4. Podemos elaborar estadísticas agregadas y verdaderamente anónimas a partir de datos ya tratados para prestar el Servicio, como el número de Organizaciones, marcas observadas, cambios detectados o informes. No creamos para ello historiales adicionales del comportamiento de los Usuarios.

9. Acceso administrativo de Organizaciones y SentioLab

Los Administradores de las Organizaciones pueden consultar operaciones administrativas relevantes, con fecha y autor. No pueden consultar el historial de inicios de sesión, direcciones IP, búsquedas ni visitas a contenidos analíticos de los empleados. El personal de SentioLab accede a los datos de clientes solo por motivos justificados de asistencia, incidentes, seguridad, facturación o exigencias legales, con autorizaciones, minimización y registros de acceso.

10. Inteligencia artificial y decisiones automatizadas

1. Gemini analiza cambios del mercado, pero no elabora perfiles de los Usuarios de MarketDrones ni de participantes en estudios grabados. No proporcionamos al proveedor de IA datos de cuentas, información de facturación, preferencias individuales ni grabaciones de procesos de solicitud.
2. No sometemos a los Usuarios a decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o les afecten de manera similar significativamente en el sentido del artículo 22 del RGPD. Para confirmar y registrar un abuso del acceso gratuito se requiere la revisión apropiada de una persona autorizada.
3. El contenido generado por IA puede contener errores y no debe ser la única base de decisiones empresariales importantes.

11. Derechos de las personas interesadas

Con las condiciones del RGPD, las personas interesadas pueden ejercer los derechos de acceso, rectificación, supresión, limitación, portabilidad, oposición al tratamiento basado en intereses legítimos (incluidos los registros de abusos confirmados) y retirada del consentimiento. Las solicitudes se envían a info@marketdrones.net. Respondemos sin demora indebida, generalmente en un mes, con las ampliaciones permitidas por el RGPD y su correspondiente comunicación.

Las personas interesadas pueden reclamar ante el Presidente de la Autoridad Polaca de Protección de Datos (UODO): https://uodo.gov.pl/. Una solicitud puede limitarse o rechazarse cuando exista fundamento legal, en cuyo caso explicaremos los motivos.

12. Información obligatoria y opcional

Los datos necesarios para crear y autenticar una cuenta y asociarla a una Organización son indispensables para usar el Servicio. Los datos de facturación son necesarios para contratar una Suscripción de pago. El consentimiento comercial es opcional y no condiciona el acceso.

13. Modificaciones

Podemos actualizar esta Política para reflejar cambios normativos, de infraestructura, proveedores o formas de tratamiento. Las modificaciones sustanciales se comunicarán adecuadamente y conforme a la ley. Las versiones

polaca, inglesa y española deben ser coherentes; las Condiciones de uso establecen la prevalencia de la versión contractual polaca cuando sea legalmente posible.