

Privacy Policy

Version of October 27, 2026

1. Controller and contact

1. The controller of personal data processed in connection with MarketDrones is **SentioLab sp. z o.o., Nowy Kiełbów 32, 26-806 Stara Błotnica, Poland**, Polish company register **KRS 0000495860**, tax ID **NIP 7010410720**, statistical number **REGON 147082076** (the “Controller”). Correspondence address: **ul. Nowoursynowska 161 L, 02-787 Warszawa, Poland**.
2. Privacy questions and requests: info@marketdrones.net. Website: <https://marketdrones.net/>.
3. This Policy covers data associated with site visits, registration and accounts, Organisation roles, monitoring publicly accessible sources, billing, security and communications. An Organisation may act as a separate controller of information it processes for its own purposes outside the Service.

2. Data subjects and categories

People concerned	Data categories
Users, Administrators and invitees	Email address, name or user label, Organisation, role and permissions, account status, invitations, report and alert settings, watched brands, records of document acceptance and marketing preferences
Representatives and contacts of Organisations	Business contact details, correspondence, support requests and details needed to manage the agreement
People connected with billing	Company and invoice details, billing contact details, payment and settlement records, payment status; we do not collect full payment-card numbers or CVV
Site visitors and Dashboard Users	IP address, session identifiers, browser/device data needed for operation, error and technical/security event information
People appearing in monitored source materials	Incidental personal information in publicly accessible pages or documents, such as names, business roles, contact details and signatures; the Service does not aim to monitor private individuals

People concerned	Data categories
People involved in confirmed abuse of free access	Minimal identifiers needed to detect a repeated breach, the date of confirmation and reason for blocking, and possibly a short record of the review outcome

We do not engage in marketing behaviour tracking or maintain a history of the analytical materials Users browse or the searches they perform. Only security and essential administrative event records are maintained as described below.

3. Purposes and legal bases

Purpose	Legal basis under the GDPR
Registration, authentication, account management, permissions and B2B Service delivery	Article 6(1)(f) – legitimate interests in performing the agreement with the Organisation and supporting its representatives; Article 6(1)(b) may apply where the data subject is the contracting individual
Invitations, Organisation administration, logs of significant administrative actions	Article 6(1)(f) – proper administration and accountability
Invoicing, accounts and taxes	Article 6(1)(c) – legal obligations; Article 6(1)(b) or (f) where required to perform the contract
Weekly reports, alerts, account/security messages and billing notices	Article 6(1)(f) – delivering the Service to an Organisation; or (b) if the individual is the contractual counterparty
Contacts, support and complaints	Article 6(1)(b) or (f), and Article 6(1)(c) where a specific legal requirement applies
Technical operation, account security, incident detection and prevention of free-access abuse	Article 6(1)(f) – security, fraud and circumvention prevention, subject to a documented necessity and balancing assessment
Voluntary promotional email about MarketDrones and SenticLab	Article 6(1)(a) – consent, together with the Polish Electronic Communications Law marketing-consent requirements

Purpose	Legal basis under the GDPR
Collecting and presenting analysis of changes in publicly available websites and documents	Article 6(1)(f) – legitimate interest in documenting and analysing market changes, subject to proportionality assessment and personal-data minimisation
Establishing, exercising and defending claims and complying with lawful authorities	Article 6(1)(f) or (c), as applicable

Marketing consent is separate, voluntary and unchecked by default. It may be withdrawn through account settings or a link in each relevant email, immediately stopping marketing communications. Withdrawal does not affect previous lawful processing or essential service communications.

4. Sources of data

We obtain data from Users and Organisation representatives; Organisation Administrators (including invitations); technical and security events; partners processing payments; and **publicly available websites and documents** covered by MarketDrones monitoring. A document's public availability does not in itself remove personal-data protection or confer unrestricted reuse rights.

For individuals mentioned in monitored sources, the Controller must separately assess the information duties under **GDPR Article 14**, any applicable exemptions, and mechanisms for exercising data-subject rights. General information about the monitoring can be found in this Policy and by contacting us.

5. Recipients and service providers

1. Account information is accessible to authorised Users and Administrators **within the same Organisation** to the extent of their roles. An Administrator can see material administrative operations but not staff login history, IP addresses or analytical browsing/search histories.
2. Authorised SentoLab personnel may access an Organisation's data only where justified for support, incident response, security, billing or legal duties. Access is restricted to what is necessary and is logged.
3. **Primary hosting:** MikrUs, with the infrastructure identified by the Provider as being located in **Finland**. Data may also be processed by the provider of the business mailbox and transactional email, accounting and billing contractors, the online payment-link provider and technical support providers.
4. **AI analysis provider:** the **paid Google Gemini API**, using a Cloud project with active Cloud Billing and **no configured EEA-only processing region**. We submit monitored source material, **not User account details, billing information or individual User preferences**. We minimise or remove incidental personal information in monitored text before submission where possible.
5. Under the Paid Services terms, Google states that it does not use submitted prompts or outputs to improve its AI products/models. Google describes retention of prompts, context and outputs **for 55 days** for safety

and abuse monitoring. The terms and technical documentation may be updated:
<https://ai.google.dev/gemini-api/terms> and <https://ai.google.dev/gemini-api/docs/usage-policies>.

6. We disclose information to public authorities only on an appropriate legal basis. We do not sell User information to advertisers.

6. International transfers

Processing through the **Gemini API may occur outside the European Economic Area**, including countries where Google or its subprocessors operate facilities. Only material actually sent to the API is concerned, which may incidentally include personal data contained in monitored sources.

Where personal data is transferred internationally, the Controller relies on an appropriate Chapter V GDPR transfer mechanism, such as an adequacy decision or Standard Contractual Clauses with necessary safeguards. Users may request information about those safeguards using our contact address.

7. Retention periods

Data	Retention rule
Active User account, Organisation account and configuration	During use of the Service; after a Subscription ends, 90 days of restricted access, followed by deletion unless a legal exception applies
Requested account deletion	Prompt removal from active systems following an effective request, except legally mandatory information or a properly justified anti-abuse exception
Backups	Automatic rolling deletion/overwriting within 7 days ; earlier deletions must be respected after recovery
Technical and security logs and SentoLab administrative access logs	Normally 180 days , longer only for specifically documented incidents, claims or legal requirements
Organisation administrative action log	Normally 180 days ; accessible in limited form to Administrators of that Organisation
Organisation invitations	Link valid for 14 days ; unaccepted, expired or cancelled invitation data deleted 30 days after expiry or cancellation , absent a separate legal basis

Data	Retention rule
Records of acceptance of Terms and marketing consents	Until account deletion; deleted with the account except where further retention is legally required
Complaints	12 months after resolution while the account still exists; promptly deleted upon valid account deletion request except where further retention is required by law
Invoices, tax and accounting records	Only for the retention period required by applicable tax/accounting legislation
Confirmed abuse of free access	12 months from confirmation of the abuse: minimal identifiers, confirmation date and reason for the block, separately from deleted accounts, only where an appropriate legitimate-interest assessment supports continued retention
Monitored sources containing incidental personal data	For the period justified by the provision of historical monitoring and change analysis

7.1. Minimal confirmed-abuse register

1. The register is used **solely** to detect repeated attempts to evade free-access rules, and not for marketing, user-behaviour analytics or commercial profiling.
2. **Suspicion alone is not sufficient for a lasting register entry.** An authorised person must first verify the evidence, confirm the breach and record a concise reason.
3. Only the User or Organisation identifiers genuinely necessary to detect recurrence are kept. The register does not contain the person's full account profile, browsing history or full correspondence. Pseudonymous or hashed identifiers may still be personal data.
4. Entries are deleted **12 months after confirmation of the specific abuse**, unless a separate legal requirement applies. Access is restricted to authorised personnel.
5. The entry may survive account deletion only if the Controller has documented its legal basis, necessity and proportionality. The individual may ask for reconsideration and exercise the right to object and other GDPR rights.

8. Cookies, localStorage and anonymous statistics

1. The site and Dashboard use only **technical cookies and/or localStorage** for login, session management, security, functions requested by Users and interface preferences.

2. We do not deploy advertising-tracking tools, marketing pixels, non-essential analytics cookies or third-party behavioural analytics tools.
3. Blocking necessary browser storage may prevent login or some functionality.
4. We may generate **genuinely anonymous, aggregated statistics** from data already processed for operating the Service, such as counts of Organisations, watched brands, detected changes or reports. We do not create new User behaviour histories for this purpose.

9. Organisation and SentionLab administrative access

Organisation Administrators may review significant administrative operations and their dates and actors. They cannot view employees' login history, IP addresses, searches or analytical page views. SentionLab personnel access client data only for justified support, outages, security, billing or legal purposes, subject to authorisation, minimisation and access logs.

10. AI and automated decisions

1. Gemini analyses market changes, rather than profiling MarketDrones Users. We do not provide the AI provider with account details, billing information or individual preferences.
2. We do not subject Users to **solely automated decisions** producing legal or similarly significant effects within the meaning of GDPR Article 22. Confirmation and recording of abuse of free access require appropriate review by an authorised person.
3. AI-generated content may contain mistakes and should not be the sole basis for important business decisions.

11. Data-subject rights

Subject to applicable GDPR conditions, individuals have rights of access, rectification, erasure, restriction, data portability, **objection** to processing based on legitimate interests (including confirmed-abuse records), and withdrawal of consent. Requests should be sent to info@marketdrones.net. We respond without undue delay, generally within **one month**, with any GDPR-permitted extension communicated as required.

Individuals may complain to the **President of the Polish Personal Data Protection Office (UODO)**: <https://uodo.gov.pl/>. A request may be limited or refused where lawful grounds apply, in which case we will provide an explanation.

12. Mandatory and optional information

Information necessary for account creation, authentication and Organisation membership is required to access the Service. Invoice details are required for a paid Subscription. Marketing consent is **optional** and is not a condition of access.

13. Amendments

We may update this Policy to reflect legal, infrastructure, service-provider or processing changes. Material changes will be communicated appropriately and as required by law. Polish and English texts should remain aligned; the Terms of Service establish the priority of the Polish contractual version where legally permissible.