Data Processing Agreement: AI Visibility

Version 1.0 · published 12 November 2026 · Marketing Player s. r. o.

Annex to the “AI Visibility” section of the Marketing Player Terms and Conditions, under Article 28 of Regulation (EU) 2016/679 (the “Regulation”) and Section 34 of Act No. 18/2018 Coll. on Personal Data Protection. If the Slovak and English versions differ, the Slovak version prevails.

Parties

Controller: the buyer, _____, _____, Identification number _____, represented by _____ (the “controller”).

Processor: Marketing Player s. r. o., Exnárova 3134/37, 821 03 Bratislava – Ružinov, Slovakia, Company ID (IČO) 53548159, Tax ID 2121408124, VAT ID SK2121408124, registered in the Commercial Register of the Bratislava III Municipal Court, Section Sro, Insert No. 150219/B, represented by Matej Kukučka, managing director (konateľ) (the “processor”).

Article 1. Definitions and relation to the Terms

1.1 Terms used in the Regulation (personal data, processing, controller, processor, data subject, personal data breach, supervisory authority) have the same meaning here. “Terms” means the “AI Visibility” section of the Marketing Player Terms and Conditions; “AI Visibility”, “Organization”, “User” and “Customer Data” have the meaning given there. “Sub-processor” is another processor the processor engages to carry out processing for the controller.

1.2 This agreement is concluded when the controller accepts the Terms, or by signature. If it conflicts with the Terms on the protection of personal data, this agreement prevails.

Article 2. Subject and duration

2.1 The subject of this agreement is the processing of personal data contained in Customer Data by the processor on behalf of the controller while providing AI Visibility.

2.2 This agreement applies for as long as the contract for AI Visibility lasts, and after it ends until the processor has deleted or returned the personal data under Article 12.

Article 3. Nature and purpose of processing

3.1 The processor processes personal data only to provide AI Visibility to the controller: storing and displaying Customer Data; sending the controller’s prompts to AI answer engines and data providers and storing their answers; analysing answers (which brands they name, citations, sentiment); producing reports, recommendations, AI-drafted texts, digests and exports; reading data from the sources the controller connects; sending e-mails to Users; support and error correction (Terms, section 8); exporting and deleting data at the controller’s request.

3.2 Processing consists of collection, storage, organisation, retrieval, use, transfer to Sub-processors, export and erasure. It is automated; the processor makes no decisions with legal effect on data subjects.

3.3 Data subjects, categories of personal data and retention periods are listed in Annex 1.

Article 4. Controller’s obligations

4.1 The controller is responsible for having a legal basis for the processing and for informing data subjects, in particular Users and persons named in brand settings.

4.2 The controller does not enter special categories of personal data or data on criminal convictions into AI Visibility, and does not put personal data into prompts unless necessary (Terms, 5.2).

4.3 The controller's documented instructions are this agreement, the Terms and the controller's settings and actions in AI Visibility. Other instructions are given in writing (e-mail is enough).

Article 5. Processor's obligations

5.1 The processor:

a. processes personal data only on the controller's documented instructions, including with regard to transfers to third countries, unless EU or Slovak law requires otherwise; in that case it informs the controller beforehand unless the law prohibits it;

b. informs the controller without delay if, in its opinion, an instruction infringes the Regulation or other data protection law;

c. ensures that persons authorised to process personal data are bound by confidentiality, which continues after their work ends;

d. takes the technical and organisational measures in Annex 3 (Article 32 of the Regulation);

e. engages Sub-processors only under Article 7;

f. assists the controller with requests of data subjects (Article 11) and with its obligations under Articles 32 to 36 of the Regulation, taking into account the nature of processing and the information available to the processor;

g. deletes or returns personal data at the end of the contract under Article 12;

h. makes available to the controller the information needed to demonstrate compliance with Article 28 of the Regulation and allows audits under Article 13;

i. keeps a record of processing activities under Article 30(2) of the Regulation.

Article 6. Roles outside this agreement

6.1 The processor is the controller of the data it needs to run AI Visibility for itself: Users' account data used for sign-in and security, the audit log of sign-ins and security changes, billing data, and e-mail addresses that visitors leave on the public AI Visibility Check. This processing is described in the processor's privacy policy at https://marketingplayer.com/terms-and-conditions/#ai-visibility-privacy, not in this agreement.

Article 7. Sub-processors

7.1 The controller gives the processor general authorisation to engage Sub-processors. The Sub-processors engaged when this agreement is concluded are listed in Annex 2.

7.2 The processor informs the controller of an intended addition or replacement of a Sub-processor by e-mail to the owners of the Organization at least 30 days in advance. The controller may object within that period on reasonable grounds relating to data protection. If the parties do not resolve the objection, the controller may terminate the contract for AI Visibility before the change takes effect and gets back the prepaid amount for the rest of the period.

7.3 The processor imposes on each Sub-processor, by contract, data protection obligations that give at least the protection of this agreement, and remains liable to the controller for the Sub-processor’s performance.

Article 8. International transfers

8.1 Customer Data are stored in the European Union (Annex 2), except the cache of dashboard figures, which the hosting provider keeps in the USA. Some Sub-processors process data outside the European Economic Area, or can access it from there.

8.2 The processor transfers personal data outside the EEA only:

a. to a country with an adequacy decision of the European Commission, including recipients in the United States certified under the EU-U.S. Data Privacy Framework; or

b. under the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 (module 3, processor to processor), with supplementary measures where needed.

8.3 The mechanism used for each Sub-processor is stated in Annex 2.

Article 9. Security

9.1 The processor implements the technical and organisational measures in Annex 3. It may update them as long as the level of protection does not decrease.

Article 10. Personal data breach

10.1 The processor notifies the controller of a personal data breach concerning Customer Data without undue delay, and at the latest within 48 hours after becoming aware of it, by e-mail to the owners and admins of the Organization.

10.2 The notification states, as far as known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact person. Information not available at first is provided as it becomes available.

10.3 The processor takes the necessary measures to contain the breach and its consequences and assists the controller with its notification to the supervisory authority and to data subjects (Articles 33 and 34 of the Regulation). The controller decides on those notifications.

Article 11. Assistance

11.1 AI Visibility lets the controller and data subjects exercise their rights themselves:

- a personal export (anyone, Account → Your data): the person’s account, sessions, memberships, invitations, consents, their own activity and audit entries, and references to the records they authored;
- an export of the Organization or a project (owners and admins, Settings → Data);
- deletion of an account, a project or the Organization (Article 12).

11.2 Where this is not enough, the processor assists the controller with requests of data subjects within 10 days of a written request. If the processor receives a request directly from a data subject concerning Customer Data, it forwards it to the controller and does not answer it itself, unless the controller instructs otherwise.

11.3 The processor provides the information it has for the controller’s data protection impact assessment and prior consultation.

Article 12. Deletion and return at the end of processing

12.1 Before the contract ends, the controller can export Customer Data in Settings → Data: a zip archive of every table the Organization or project owns, as JSON, with the main tables also as CSV. Exports are kept for 7 days; download links are signed, expire with the export and require a signed-in owner or admin. Stored provider keys, password hashes, API key and session secrets and two-factor secrets are never exported.

12.2 Deleting the Organization (owners and admins, with typed confirmation) stops tracking at once and e-mails every owner and admin; after a 7-day grace period, which an owner may use to cancel, every project and every Organization-level record (members, invitations, keys, settings, activity log) is deleted. Deleting a project deletes all its records, including answers, citations, analytics, settings and usage. Deletion also removes queued background jobs and cached dashboard results.

12.3 If the contract ends and the controller has not deleted the Organization, the processor deletes Customer Data within 30 days after the end of the contract, unless the controller asks for its return first. For an Organization whose Trial ended without a Package, the deletion in section 2.3 of the Terms applies.

12.4 After deletion the following remain:

a. audit log entries (exports, deletions, team, role and key changes), without IP addresses, kept 2 years from their creation;

b. deleted data in database backups until the backups expire under the database provider’s backup window (under the provider’s plan, by default 7 days);

c. data the processor must keep under the law.

12.5 On request, the processor confirms the deletion in writing.

Article 13. Audits

13.1 The processor provides the controller, on request, with the information needed to demonstrate compliance with this agreement, primarily this agreement and its annexes and the Sub-processors’ certifications and reports where available.

13.2 If that information is not enough, the controller or an auditor bound by confidentiality may carry out an audit, at most once in 12 months and additionally after a personal data breach, on 30 days’ written notice, during business hours, without access to other customers’ data and at the controller’s cost. Audits of Sub-processors are carried out through the reports they make available.

Article 14. Liability

14.1 Each party is liable for damage caused by breach of this agreement under the Regulation and Slovak law. As between the parties, the processor’s liability under this agreement is subject to the limitation in section 9 of the Terms (Liability), including the cap of the amount the controller paid for AI Visibility in the 12 months before the event that caused the damage, to the extent the law allows. The limitation does not affect the rights of data subjects under Article 82 of the Regulation.

Article 15. Final provisions

15.1 This agreement is governed by the law of the Slovak Republic; disputes are decided by the courts of the Slovak Republic.

15.2 The processor may change this agreement in the way set out in section 12.1 of the Terms. Changes required by law or by a supervisory authority take effect when the law or the authority requires.

15.3 If the Slovak and English versions differ, the Slovak version prevails.

Controller: _____, _____

Processor: _____, Matej Kukučka, konateľ / managing director, Marketing Player s. r. o.

_____

Annex 1. Description of processing

Data subjects: Users (the controller's employees, contractors and agency staff with an account); people invited to the Organization; people named in brand settings (for example the brand's leaders in a fact sheet); people named in AI answers when a prompt asks about them.

Categories of personal data:

Data	Contents	Personal data
Accounts	Name, e-mail, password hash or a Google sign-in link, sessions with IP address and browser, optional two-factor secret and backup codes	Yes
Organization and team	Members and their roles, invitations (invitee e-mail), API keys (hashed), per-project access	Members' names and e-mails
Brand settings	Websites, competitors, prompts, markets, fact sheets, notes, tasks, content records	Authors of notes, tasks and facts; people a fact sheet names
AI answers	Prompts sent to answer engines, answers, citations, products, derived mentions and sentiment	Normally none; an answer can name people when a prompt asks about them
Connected analytics	Aggregated Search Console, GA4, Usermaven and Bing figures per day, page and query; crawler visits per bot and page	Aggregates only, no visitor-level data
Activity log	Who changed what in the dashboard	Users' names
Audit log	Exports, deletions, team, role and key changes, password and two-factor changes, support access	Users' names, IP addresses, browser
Exports	Archives built at the controller's request	As the exported data

No special categories of personal data are processed.

Retention:

Data	Kept
Account, Organization and project data	Until deleted by the controller (Article 12)
Answers in detail (text, mentions, citations, names, products)	13 months, except the answers a task, an annotation, a "Did it work?" plan, a content page or a split test still reads, and each prompt's newest answer
Aggregated trends (visibility, share of voice, sentiment, cited pages)	As long as the project exists

Data	Kept
Raw responses of the answer engines, moved to file storage after 30 days	13 months
Search Console and Bing figures per day	16 months
Crawler visits per day	13 months, then as monthly totals
Sessions	Until they expire or the User signs out
Activity log	180 days
Audit log	2 years, append-only; a deleted person’s entries are kept as “Deleted user” without IP addresses
Exports	7 days
Cached dashboard results	At most 7 days; a deleted project’s entries are removed within an hour
Organization scheduled for deletion	7 days’ grace, then deleted
Organization whose Trial ended without a Package	60 days after the Trial ended, after a warning on day 53
Organization that had a subscription, after it ends	Until the controller deletes it; nothing deletes it automatically (Article 12.3)
Database backups	Under the provider’s plan, by default 7 days

Annex 2. Sub-processors

#	Sub-processor	Activity	Personal data concerned	Location	Transfer mechanism
1	Supabase (Supabase Pte. Ltd., Singapur / Singapore)	Database and job queue for all Customer Data	All categories in Annex 1	Frankfurt, Germany (AWS eu-central-1); support may access from outside the EEA	Stored in the EU; for access from outside the EEA SCCs (2021/914)
2	Netlify (Netlify, Inc., USA)	Hosting of the dashboard and its server functions; cache of dashboard figures (Netlify Blobs), at most 7 days	All categories while displayed	Functions and Blobs: Ohio, USA (us-east-2)	SCCs (2021/914) and EU–US Data Privacy Framework
3	GitHub (GitHub, Inc., USA), GitHub Actions	Nightly processing: runs the worker that reads and writes the database; nothing is kept on the runner after a run	All categories, during a run	USA (GitHub-hosted runners on AWS or Microsoft Azure)	SCCs (2021/914) and EU–US Data Privacy Framework
4	Resend (Plus Five Five, Inc. (Resend), USA)	Transactional e-mail: invitations, password resets, digests, export, deletion and Trial notices	Users’ names and e-mails, e-mail contents	USA	SCCs (2021/914) and EU–US Data Privacy Framework

#	Sub-processor	Activity	Personal data concerned	Location	Transfer mechanism
5	Sentry (Functional Software, Inc. (Sentry), USA)	Error reports from the dashboard and the worker, scrubbed of e-mail addresses, credentials, query strings and request bodies; IP addresses not stored	A User only as an opaque id; technical data	EU (Frankfurt) for error reports; accounts and organisation settings in the USA	SCCs (2021/914) and EU–US Data Privacy Framework
6	Usermaven (Usermaven Inc.), only if switched on for the dashboard	Product analytics of the dashboard's own pages	Visitor identifier, pages visited	Germany (EU, Hetzner Online GmbH); limited access outside the EEA for support, billing, communications and optional AI features (TIA v1.1)	SCCs (2021/914)
7	DataForSEO (DataForSEO OÜ, Estónsko / Estonia)	Sends tracked prompts to AI answer engines and search, returns answers; search results and keyword volumes	Prompt text with the market's country and language; answers	Company in Estonia (EU), servers not stated	SCCs (2021/914) or an adequacy decision
8	Anthropic (Anthropic Ireland, Limited)	Claude answers, onboarding research, Opportunities report, Ask your data, AI-drafted articles, fallback mention judge	Prompts, the brand's website text, brand settings, Users' questions, answers	USA	SCCs (2021/914)
9	Google (entity per cloud.google.com/terms/google-entity), Gemini API, paid tier	Lists the organisations every answer names and checks its claims against the fact sheet; embeddings; reads the brand's home page and cited pages; fallback mention judge	Every answer's text with its prompt; the brand's name, aliases and fact sheet; texts of the brand's own pages and cited pages; phrases taken from answers	Countries where Google has facilities; the Gemini API makes no EU-only processing commitment	SCCs (2021/914) and EU–US Data Privacy Framework
10	Typesafe (Jev) (being verified)	Judges whether answers name the brand and its competitors, and in what tone; only answers that name one of them are sent	Answer texts with their prompts, brand and competitor names	Being verified	Being verified

#	Sub-processor	Activity	Personal data concerned	Location	Transfer mechanism
11	Stripe (Stripe Payments Europe, Limited)	Subscriptions, payments and invoices	The Organization's name; billing address, VAT ID and payment details the payer enters at Stripe; billing data, for which the processor is controller (Article 6)	EU and USA (Stripe, LLC)	SCCs (2021/914) and EU–US Data Privacy Framework

Services that are not Sub-processors. The following receive no personal data from AI Visibility, or are reached with the controller's own account and grant: Google Search Console, Google Analytics 4 and Google Analytics Admin (read with the controller's grant; only aggregates are stored), Bing Webmaster Tools and the controller's own Usermaven workspace (read with the controller's key), Ahrefs (domains, keywords), Google Keyword Planner, Chrome UX Report (page addresses), YouTube and Google Knowledge Graph (brand names), GDELT (brand and competitor names), Wikimedia (company names), IndexNow (the brand's own page addresses).

Annex 3. Technical and organisational measures

1. **Encryption in transit:** TLS on every connection between Users, the dashboard, the database and every Sub-processor.
2. **Encryption of keys:** provider keys and other secrets that an Organization stores are encrypted at rest in the application and are sent only to the provider they belong to. Passwords and API keys are stored only as hashes.
3. **Database access:** a dedicated database project in Frankfurt, reached only by the application under its own role. The database provider's public data API is closed; the public roles have no access to the application's schema, and every table has row-level security with no policies, so no other role can read it.
4. **Access control:** every request checks the User's membership and role in the Organization and their access to the project. Optional two-factor sign-in for password accounts. Sign-in and public endpoints are rate-limited.
5. **Support access:** the processor's staff open an Organization read-only by default, write access is time-boxed to 60 minutes, sensitive actions stay with the Organization's members, provider keys stay masked, and every visit is written to the Organization's audit log.
6. **Logging:** an append-only audit log of exports, deletions, team, role and key changes, password and two-factor changes and support access, visible to the Organization's owners and admins; an activity log of changes in the dashboard.
7. **Data minimisation in error reports:** before an error report leaves the application, e-mail addresses, sign-in and cookie headers, keys and tokens, credentials in query strings and connection-string passwords are removed; request bodies are never sent; the error monitoring stores no IP addresses and accepts events only from the deployment's own domain.
8. **Exports:** built in the background, available only through signed links that expire with the export and require a signed-in requester (for an Organization, an owner or admin); secrets are never included; every request and download is logged.
9. **Deletion:** which records each deletion and export covers is defined in one place in the code, and an automated test fails when a new table that refers to a project, an Organization or a person is not covered.
10. **Retention:** a daily job deletes data past the periods in Annex 1.

11. **Organisational measures:** only the processor’s managing director has production access to the application (Super admin). An AI development tool (Claude, Anthropic) has read-only access to the database, under the processor’s control..