rankscan

rankscan.ai

AGREEMENT · DATA PROTECTION

Data Processing Agreement

under Art. 28 GDPR and Art. 9 FADP, with the Standard Contractual Clauses of the European Commission

CONTROLLER

The Customer, as specified in the RankScan Customer Account

PROCESSOR

Klarplan AG, Sälihalde 11, 6005 Lucerne, Switzerland, provider of RankScan

VERSION

1.2 of 28 October 2026

CURRENT VERSION

rankscan.ai/data-processing-agreement

Contents

Part A – Framework Provisions 3
- A.1 Definitions 3
- A.2 Application, Term and Versions 3
- A.3 Order of Precedence 4
- A.4 Subject Matter and Roles 4
- A.5 Instructions (re Clause 7.1) 6
- A.6 Swiss Data Protection Law 6
- A.7 Evidence and Audits (re Clause 7.6) 7
- A.8 Sub-processors (re Clause 7.7) 7
- A.9 End of the Plan, Dormant Period, Return and Deletion (re Clause 10(d)) 7
- A.10 Export, Individual Data and Data Subject Requests (re Clause 8) 9
- A.11 Liability 10
- A.12 Governing Law, Place of Jurisdiction and Language 10

Part B – Standard Contractual Clauses 11
- Section I 11
- Section II – Obligations of the Parties 12
- Section III – Final Provisions 16

Annex I – List of Parties 17

Annex II – Description of the Processing 18
- 1. Delimitation by Operation 18
- 2. Categories of Data Subjects 18
- 3. Categories of Personal Data 19
- 4. Sensitive Data (re Clause 7.5) 19
- 5. Nature of the Processing 20
- 6. Purposes 20
- 7. Duration of the Processing 20
- 8. Processing by Sub-processors 21

Annex III – Technical and Organisational Measures 22

Annex IV – List of Sub-processors 26
- Services without Processing on Behalf 32

Data Processing Agreement (DPA) RankScan between the Customer (controller) and Klarplan AG, Sälihalde 11, 6005 Lucerne, Switzerland, provider of RankScan (processor).

This Agreement consists of two parts. Part A supplements the Standard Contractual Clauses. Part B contains the Standard Contractual Clauses of the European Commission under Art. 28(7) GDPR (Implementing Decision (EU) 2021/915) with Annexes I–IV.

PART A

Framework Provisions

Part A supplements Part B in accordance with Clause 2(b). No provision of Part A shall be interpreted in a way that directly or indirectly contradicts Part B or detracts from the rights of data subjects.

A.1 Definitions

1. **Service Agreement:** the agreement on the use of RankScan under the General Terms and Conditions of Klarplan AG (GTC). It begins with registration and ends with the deletion of the Customer Account.
2. **Customer Account:** the Customer's account in RankScan with its websites (properties), team members and data.
3. **Team Members:** all persons with access to the Customer Account. Their roles are Owner, Admin and Member. The Owner is the person registered as owner in the Customer Account. The Owner always has the rights of an Admin. If a Customer Account has no Owner, an Admin exercises the Owner's rights under this Agreement.
4. **Plan:** a current paid subscription, a current trial period or a plan that Klarplan AG has agreed individually with the Customer.
5. **Trial Account:** a Customer Account whose only Plan was a trial period.
6. **Dormant Period:** the time during which a Customer Account exists without a Plan (A.9 para. 2).
7. **Customer Data:** the personal data that Klarplan AG processes on behalf of the Customer in accordance with Annex II.
8. **Sub-processor:** a sub-processor within the meaning of Clause 7.7. The agreed list is Annex IV.
9. **Superadmin:** a person at Klarplan AG with access to all Customer Accounts for operations and support.

A.2 Application, Term and Versions

1. This Agreement applies to every Customer to the extent that Klarplan AG processes Customer Data on its behalf. It forms part of the Service Agreement. It takes effect upon acceptance of the GTC at registration. For Customers who registered before the publication of the first version, para. 8 applies.
2. On request, Klarplan AG provides a signed version. Its content is identical.
3. This Agreement remains in force until Klarplan AG has deleted all Customer Data in accordance with A.9. For remaining data under A.9 para. 7, it remains in force until their deletion. The end of a Plan does not terminate it.

4. Each version bears a number and a date. The current version is available at https://rankscan.ai/data-processing-agreement (German original: https://rankscan.ai/de/data-processing-agreement). Klarplan AG provides earlier versions on request.
5. Klarplan AG does not amend Part B. Changes to Annex IV are governed by Clause 7.7(a) and A.8.
6. Klarplan AG announces changes to Part A and Annexes I–III at least 30 days in advance by e-mail to the Owner and the Admins. The announcement states the day on which the change takes effect. The Customer may object in text form until that day. If the Customer does not object, the change takes effect for the Customer on that day. If the Customer objects, the previous version continues to apply to the Customer. Klarplan AG may then terminate the Service Agreement in accordance with the GTC. A change that reduces the protection of Customer Data takes effect only with the Customer's consent in text form.
7. Para. 6 conclusively governs how amendments to this Agreement take effect. The rule in the GTC under which silence counts as consent to amended GTC does not apply to this Agreement.
8. **Existing Customers.** For Customers who registered before the publication of the first version of this Agreement, the following applies:

   8.1 Klarplan AG sends this Agreement by e-mail to the Owner and the Admins and asks the Customer to expressly accept it in text form within 30 days of receipt, for example by e-mail to hello@rankscan.ai. The notice states the end of this period.

   8.2 This Agreement takes effect upon receipt of the Customer's express acceptance by Klarplan AG, unless the parties agree on a later start. Silence or mere continued use of RankScan does not replace acceptance. Klarplan AG documents the acceptance and the version accepted.

   8.3 If the Customer rejects the Agreement or does not accept it within the period under para. 8.1, Klarplan AG may terminate the Service Agreement in accordance with the GTC. Existing statutory and contractual data protection obligations remain unaffected.

A.3 Order of Precedence

In the event of a conflict, the following order of precedence applies: Part B with Annexes I–IV, then Part A, then the GTC. The Privacy Policy governs only the processing for which Klarplan AG is itself the controller.

A.4 Subject Matter and Roles

1. Klarplan AG processes Customer Data only for the purposes set out in Annex II, Section 6.
2. Annex II, Section 1 determines for which operations Klarplan AG acts as processor and for which it is itself the controller. The operation is decisive, not the category of data.
3. **Third-party websites.** The Customer determines which websites, competitors, keywords and prompts RankScan monitors. For this purpose, RankScan also processes public third-party content: competitors' websites, search results, answers from AI assistants and pages cited in those answers. This processing is carried out on behalf of the Customer. The Customer ensures that it is permitted to have the content analysed and that a legal basis exists for the processing.

4. **Customers acting on behalf of others.** If the Customer uses RankScan to process data for which a third party (End Customer) is the controller, the following applies in addition:

   4.1 The Customer acts as processor towards the End Customer. Klarplan AG is its sub-processor (Art. 28(4) GDPR, Art. 9(3) FADP). This Agreement is then the contract between processor and sub-processor. The rights that Part B grants to the controller are exercised by the Customer towards Klarplan AG. The Customer's obligations towards the End Customer remain unaffected.

   4.2 The Customer warrants that its instructions correspond to the End Customer's instructions and that the End Customer has approved the engagement of Klarplan AG and of the sub-processors listed in Annex IV.

   4.3 Klarplan AG accepts instructions only from the Customer. It addresses notices under Part B to the Customer. The Customer forwards them to the End Customer.

   4.4 Audits and information for the End Customer are requested by the Customer. An End Customer may accede to this Agreement under Clause 5.

5. **Microsoft Copilot on the Customer's instruction.**

   5.1 If the Customer selects the AI assistant Microsoft Copilot for a website, it instructs Klarplan AG to transmit the prompts of that website to the Microsoft Copilot service via the technical integration provider cloro (Annex IV no. 7).

   5.2 Microsoft processes and answers the prompts as an independent controller under the terms of use and privacy provisions applicable there. Microsoft is not a sub-processor of Klarplan AG; there is no contractual relationship between Klarplan AG and Microsoft. The forwarding to Microsoft constitutes a disclosure of data by the Customer to a third party. For this disclosure, the Customer ensures its own legal basis under the GDPR or justification under the FADP, where required. Microsoft typically also processes data outside Switzerland and the EU/EEA (in particular in the USA).

   5.3 Under its own terms, Microsoft reserves the right to use transmitted prompts to provide, analyse and develop its own services or to have them reviewed by personnel. Klarplan AG has no influence on the retention period, further processing or deletion of data at Microsoft and can neither initiate nor verify deletion there.

   5.4 The technical query is made via cloro as an intermediary service. cloro submits the requests via the publicly accessible interface of Microsoft Copilot. cloro does not contractually guarantee the query path and does not announce technical adjustments in advance. The Customer decides on its own responsibility whether to initiate a query via cloro despite these conditions and Microsoft's terms of use. Klarplan AG may discontinue queries via Microsoft Copilot at any time.

   5.5 Microsoft Copilot is deemed a restricted AI assistant under para. 6. RankScan points out the characteristics under paras. 5.2 to 5.4 at the time of selection.

   5.6 The Customer may deactivate the selection of Microsoft Copilot for each website at any time with effect for the future. Thereafter, no further prompts of that website are transmitted to Microsoft Copilot.

6. **Restricted AI assistants.**

   6.1 Klarplan AG designates an AI assistant in Annex IV as "restricted" if its provider or the recipient of the prompts is located in a country without adequate data protection and no recognised safeguard exists for the disclosure from Switzerland or for the transfer from the EU; it suffices that one of the two is missing. An AI assistant whose recipient receives the prompts as an independent controller is also restricted.

   6.2 The Customer does not enter personal data in prompts for restricted AI assistants. This obligation is a contractual rule, not a technical block.

   6.3 RankScan marks restricted AI assistants at the time of selection for each website and when prompts are entered, and points out the obligation under para. 6.2.

   6.4 Restricted AI assistants receive prompts only if the Customer selects them itself. They are not part of the default selection.

   6.5 Klarplan AG announces changes to the designation in accordance with A.8 para. 6.

A.5 Instructions (re Clause 7.1)

The following are deemed documented instructions within the meaning of Clause 7.1:

1. the GTC and this Agreement,
2. the Customer's settings and actions in RankScan, in the Reporting API and in the MCP server. Examples: monitored websites, keywords, prompts, competitors, the selection of AI assistants per website, the connection of Search Console and Google Analytics 4, team members, recipients of notifications and shared reports, delegated measures and the deletion of data,
3. further instructions from the Owner or an Admin in text form to hello@rankscan.ai. Klarplan AG retains these instructions.

A.6 Swiss Data Protection Law

To the extent that the processing is subject to the Swiss Federal Act on Data Protection (FADP), the following applies in addition:

1. References in Part B to Regulation (EU) 2016/679 are also deemed references to the corresponding provisions of the FADP, in particular Art. 9 FADP (processing by processors).
2. "Supervisory authority" includes the Federal Data Protection and Information Commissioner (FDPIC).
3. "Member State law" includes Swiss law.
4. "Third country" means, for disclosures from Switzerland, a country without adequate protection under Art. 16 FADP. References to Chapter V of Regulation (EU) 2016/679 are deemed references to Art. 16 and 17 FADP for such disclosures.
5. The general authorisation under Clause 7.7(a) is the prior authorisation under Art. 9(3) FADP.
6. Notifications under Clause 9 are made in such a way that the Customer can fulfil its obligation under Art. 24 FADP.

A.7 Evidence and Audits (re Clause 7.6)

1. Klarplan AG demonstrates compliance primarily by means of documents: this Agreement, Annex III, the list of sub-processors and, on request, further information.
2. The Customer may conduct or commission an audit under Clause 7.6(c) and (d) at reasonable intervals, as a rule no more than once per calendar year. If there are indications of non-compliance, an audit is possible at any time.
3. The Customer announces an audit at least 30 days in advance in text form. If there are indications of non-compliance, a reasonable shorter period applies.
4. A mandated auditor is bound to confidentiality and is not a competitor of Klarplan AG.
5. Each party bears its own costs of the audit.

A.8 Sub-processors (re Clause 7.7)

1. The agreed list under Clause 7.7(a) is Annex IV in the version published at https://rankscan.ai/subprocessors.
2. Klarplan AG informs the Owner and the Admins by e-mail at least 30 days before adding or replacing a sub-processor. The notice states name, address, activity, data, place of processing and transfer basis. At the same time, Klarplan AG announces the change on the page referred to in para. 1, stating the date from which it applies. Only from that date does the new sub-processor form part of the agreed list.
3. The Customer may raise a reasoned objection in text form within this period. The parties then seek a solution, for example waiving the affected function for this Customer Account. Until a solution is found, Klarplan AG does not disclose Customer Data of this Customer Account to the new sub-processor, insofar as the service can be separated per Customer Account. This is the case for services that RankScan selects per Customer Account or per website, for example the AI assistants of AI Visibility. It is not the case for shared infrastructure such as database, server or e-mail delivery.
4. If the parties find no solution or the service cannot be separated per Customer Account, the Customer may terminate the Service Agreement as of the date of the change. Klarplan AG refunds prepaid fees for the period thereafter on a pro rata basis. The exclusion of refunds in the GTC does not apply in this case.
5. The Customer selects the AI assistants of AI Visibility per website. Without a selection of its own, a default selection according to Annex IV applies. If the Customer deselects a provider, no new prompts of that website are sent to it. Restricted AI assistants (A.4 para. 6) are not part of the default selection.
6. Other changes to Annex IV, for example new categories of data at a provider or a changed default selection, are announced by Klarplan AG in accordance with A.2 para. 6.
7. The sub-processors' contracts are named in Annex IV.

A.9 End of the Plan, Dormant Period, Return and Deletion (re Clause 10(d))

1. **End of the Plan.** A subscription ends in accordance with the GTC, for example by termination at the end of the billing period. A trial period ends on its expiry. An individually agreed Plan ends in accordance with that agreement. The Customer Account and the Service Agreement thereafter continue in the Dormant Period.

2. **Dormant Period.** The basis of the Dormant Period is this Agreement as the Customer's instruction. The Customer may end it at any time in accordance with para. 3.

   2.1 **Start:** the day on which the last Plan ends.

   2.2 **End:** a new Plan ends the Dormant Period. A login does not end it. Otherwise, Klarplan AG deletes the Customer Account 12 months after the start of the Dormant Period, a Trial Account 3 months after the start.

   2.3 **Reminder:** 30 days before deletion, the Owner receives an e-mail stating the deletion date and referring to export and deletion under paras. 3 and 4. Without an Owner, it goes to the Admins; without Admins, to all Team Members. Deletion takes place no earlier than 30 days after the reminder. If the reminder is sent later, the deletion is postponed accordingly.

   2.4 **Permitted processing:** storage; deletion according to the periods in Annex II; the reminder; export, deletion and resumption on instruction; support.

   2.5 **No longer processed:** Klarplan AG does not start any scans, does not retrieve Search Console, Google Analytics 4 or the Chrome UX Report and does not send any requests to language models or search services. Jobs that began before the end of the Plan run to completion. Notifications already triggered may still be sent.

   2.6 **Access:** Without a Plan, the Customer has no access to the data in the application or via the Reporting API. The Owner sees only the plan selection or a blocking page. Return therefore takes place via the export under A.10 para. 2.

3. **Earlier deletion on instruction.** The Customer may request deletion at any time.

   3.1 With a Plan, the Owner deletes the Customer Account itself in the settings, using its password.

   3.2 Without a Plan or without an Owner, the Owner or an Admin (A.1 para. 3) writes to hello@rankscan.ai from the e-mail address stored in the Customer Account. Klarplan AG deletes the Customer Account within 10 working days of the request.

   3.3 Individual websites are deleted by an Admin (A.10 para. 4).

4. **Return and choice under Clause 10(d).** Until deletion, the Customer may request the export under A. 10 para. 2, including after the end of the Plan and during the Dormant Period. The Customer chooses return followed by deletion, or deletion only. If the Customer makes no choice by the end of the Dormant Period, Klarplan AG deletes the data. After deletion, return is no longer possible.

5. **Deletion process.** Deletion immediately blocks the Customer Account and removes all Team Members. A background job then deletes all Customer Data in accordance with Annex III ("Deletion"). Together with the Customer Account, Klarplan AG deletes the user accounts that belong to no other Customer Account, including profile pictures.

6. **Confirmation.** After completion of the deletion, the Owner automatically receives a confirmation by e-mail. Without an Owner, the following applies:

   6.1 If Klarplan AG deletes at the request of an Admin (para. 3.2), it confirms the deletion to that Admin in text form after completion.

   6.2 If it deletes after expiry of the Dormant Period, it confirms the deletion automatically by e-mail: to the Admins; without Admins, to all former Team Members (para. 2.3).

7. **Remaining data.** After deletion, only the following remain:

   7.1 copies in backups until their expiry, at the latest 35 days after deletion (Annex III). For backup copies of the test environment, para. 7.3 applies instead. Klarplan AG uses the backups only to restore the entire system. If it restores a backup, it deletes the affected data again before using the backup for operations or tests.

   7.2 entries in logs and technical queues: application logs for up to 14 days, failed background jobs in the queue for up to 7 days, the audit log for up to 365 days. Klarplan AG uses them only for security, evidence and troubleshooting.

   7.3 the copy in the test environment until its next refresh. Klarplan AG rebuilds the test environment at least every 30 days, and after a deletion on request within 10 working days at the latest. From the deletion of the Customer Account, it no longer performs tests or provider calls for that account's data in the test environment. After removal from the test environment, copies exist in automatic daily backups for at most 7 days and in manual snapshots for at most 30 days longer (Annex III). These backup copies therefore exist for at most 60 days in total after the deletion of the Customer Account. Para. 7.1 applies to their use and to any restoration.

   7.4 the authorisation to access Search Console and Google Analytics 4 in the Customer's Google account. Deletion removes the credentials in RankScan but does not revoke the authorisation at Google. The Customer may revoke it in its Google account. If the Customer disconnects Search Console or Google Analytics 4 before deletion, RankScan revokes the authorisation itself, provided that the Customer Account holds no other Google access.

8. Data for which Klarplan AG is itself the controller (Annex II, Section 1) are governed by the Privacy Policy.

A.10 Export, Individual Data and Data Subject Requests (re Clause 8)

1. **Reporting API.** While a Plan is in place, an Admin creates a token for the Customer Account. Via the Reporting API, the Customer retrieves analyses, for example scores, rankings and AI visibility. It does not provide all Customer Data.

2. **Full export.** At the Owner's request, Klarplan AG creates an export of the Customer Account within 10 working days. The export is free of charge, including during the Dormant Period. The export is a ZIP file with one JSONL file per table, an overview (manifest), the profile pictures of the Team Members and the screenshots of support requests. It also contains the internal triage of support requests (category, urgency, summary, draft reply). Not included are:

   2.1 credentials and tokens, because they would open the account,

   2.2 billing data and cost counters, because Klarplan AG is itself the controller for them,

   2.3 usage analytics, because Klarplan AG is itself the controller for them (Privacy Policy),

   2.4 working data of running crawls, because they exist only until the end of a run.

3. **Delivery.** Klarplan AG sends a signed download link to the Owner's e-mail address stored in the Customer Account. The link is valid for 7 days and requires no login. Anyone who has the link can download the file. The Customer therefore keeps it confidential. Klarplan AG deletes the file at the latest on the day after the link expires. Deletion of the Customer Account also deletes the export.

4. **Rectification and deletion by the Customer.** While a Plan is in place, the Customer itself modifies or deletes:

   4.1 Team Members, invitations and recipients of notifications (Admin),

4.2 websites and all scans of a dimension (Admin),

4.3 topics, keywords, prompts, competitors and contacts for delegated measures (all Team Members).

Together with a website, a keyword, a prompt or a competitor, RankScan deletes the associated results. Each user modifies and deletes their own profile themselves, including without a Plan. The Owner must first transfer or delete the Customer Account to do so; without a Plan, in accordance with A.9 para. 3.

5. **Content without individual deletion; support requests.**

5.1 Individual crawled pages, search results and AI answers cannot be individually deleted or rectified by either the Customer or Klarplan AG using a designated procedure. RankScan stores them as delivered by the source. Klarplan AG does not search this content specifically for individual persons.

5.2 This content lapses after the periods in Annex II or upon deletion of the prompt, the keyword, the website or the Customer Account. The Customer carries out this deletion itself in accordance with para. 4. Without a Plan, Klarplan AG deletes on instruction in accordance with A.9 para. 3.

5.3 A Superadmin deletes an individual support request on the Customer's instruction within 10 working days of receipt of the instruction. The instruction is given by the Owner or an Admin in text form to hello@rankscan.ai (A.5 para. 3). Deletion covers text, history, screenshots and the internal triage of the request. The Superadmin states a reason, which is recorded in the audit log. Copies in backups continue to exist until their rotation, at the latest 35 days after deletion (Annex III). Klarplan AG uses them only to restore the entire system.

6. **Data subject requests.** If Klarplan AG receives a request concerning Customer Data, it forwards it to the Owner without undue delay, at the latest within 5 working days. The maximum period does not permit any delay where earlier forwarding is possible. Klarplan AG does not answer the request itself unless the Customer authorises it to do so. Requests concerning data for which Klarplan AG is itself the controller are answered by Klarplan AG.

A.11 Liability

1. Liability is governed by the GTC, unless mandatory law and Part B provide otherwise.
2. The exclusion of liability for third-party providers in the GTC does not apply to the sub-processors under Annex IV. For them, Klarplan AG is liable in accordance with Clause 7.7(d).
3. The rights of data subjects, in particular under Art. 82 GDPR, remain unaffected.

A.12 Governing Law, Place of Jurisdiction and Language

1. Part A is governed by Swiss law. The place of jurisdiction is Lucerne. Mandatory places of jurisdiction and the rights of data subjects and supervisory authorities under the GDPR and the FADP are reserved.
2. This Agreement is available in German and English. In the event of discrepancies, the German version prevails.

PART B

Standard Contractual Clauses

Commission Implementing Decision (EU) 2021/915. The wording is adopted unchanged.

Section I

Clause 1: Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2: Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional: Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Section II – Obligations of the Parties

Clause 6: Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7: Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or ac-

cess to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8: Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject.

It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9: Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III – Final Provisions

Clause 10: Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of Parties

Re Clause 1(b) and Clause 5.

Item	Controller	Processor
Name	the Customer, as specified in the RankScan Customer Account	Klarplan AG (RankScan)
Address	as specified in the Customer Account or in the billing address	Sälihalde 11, 6005 Lucerne, Switzerland
Contact person	Owner of the Customer Account (Owner's e-mail address)	René Häfliger, Member of the Board and Managing Director, hello@rankscan.ai
Data protection advisor / officer	–	none appointed; requests to hello@rankscan.ai
Representative in the EU under Art. 27 GDPR	–	none appointed
Signature and accession date	acceptance of the GTC at registration; for Existing Customers, the start under A.2 para. 8.2; for a signed version, signature and date	publication of this Agreement; for a signed version, signature and date

If the Customer acts on behalf of an End Customer under A.4 para. 4, it is the processor of the End Customer. It exercises the rights of the controller under these Clauses in accordance with A.4 para. 4.1.

ANNEX II

Description of the Processing

Re Clause 6.

1. Delimitation by Operation

Operation	Role of Klarplan AG	Governed by
Content and analyses: crawl of the Customer's websites, Search Console and Google Analytics 4 data, search results, AI visibility, competitors, measures, summaries, reports, weekly report, shared reports, delegated measures, notifications	processor	this Agreement
Team management by the Customer: who has access, roles, invitations, recipients of notifications and reports, contacts for delegated measures	processor	this Agreement
User account and login: registration, login, password, protection against abuse	controller	Privacy Policy
Application and audit logs (security, evidence)	controller	Privacy Policy
Support: content of the request and screenshots, insofar as they contain Customer Data	processor	this Agreement
Support: exchange with the Customer as contracting party (sender, history)	controller	Privacy Policy
Billing, payments, commissions to intermediaries	controller	Privacy Policy
Usage analytics of the application	controller	Privacy Policy
Own e-mails, conversion measurement, website rankscan.ai	controller	Privacy Policy

2. Categories of Data Subjects

- Team Members of the Customer and invited persons
- recipients of notifications and shared reports
- external contacts to whom the Customer delegates measures, for example employees of a web agency
- persons named in the Customer's support requests
- persons whose name or contact details appear on public websites that RankScan processes on behalf of the Customer: the Customer's websites, those of its competitors and pages cited in AI answers (for example contact persons, authors, owners of sole proprietorships)
- persons named in search results, answers from AI assistants or Search Console queries
- persons whose names the Customer enters in prompts, competitors or notes

3. Categories of Personal Data

- name, e-mail address and role of Team Members, invited persons, recipients and external contacts
- content of public web pages: text, headings, titles, links, metadata, image URLs
- data from the Customer's Google Search Console: pages, clicks, impressions, click-through rate, position, the most frequent queries per page and results of the URL inspection. The values are aggregated and contain no data on individual visitors. Queries may contain the names of persons searched for.
- data from the Customer's Google Analytics 4: sessions, page views, visit duration and number of selected events per landing page, day and source. The values are aggregated and contain no data on individual visitors.
- prompts, keywords, competitors, positioning and answers from the strategy dialogue, notes
- search results and answer texts from AI assistants for the Customer's prompts, including the names mentioned in them
- free text on measures and comments from external contacts
- subject, text, page URL and screenshots of support requests

4. Sensitive Data (re Clause 7.5)

1. **Intended:** none. RankScan is not intended for the processing of sensitive data.
2. **Where they may occur incidentally:** in the content of public web pages, in search results, answers from AI assistants and Search Console queries, in prompts, keywords and notes, and in support requests.
3. **Technical limits:** RankScan does not detect sensitive data and does not filter them out. What the Customer or a website delivers, RankScan processes within the scope of Annex II, including the transfer to sub-processors under Annex IV.
4. **Restrictions and safeguards that apply:**

- RankScan does not analyse content by person and does not build profiles of persons.
- RankScan crawls only publicly accessible pages and respects robots.txt.
- RankScan does not send the text of crawled pages stored in RankScan to any language model. The exception is the page title: for meta description suggestions, in the review of measures and in content briefs. For the strategy dialogue and the review of cited pages, RankScan retrieves page text separately and sends it to the providers under Annex IV.
- Screenshots of support requests are not sent to any language model. Users' free text on skipped measures is not sent to the review of measures.
- RankScan reduces raw crawl data to aggregated values after 14 days.
- Access by Klarplan AG personnel in accordance with Annex III, with audit log.

5. **Obligations of the Customer:** The Customer does not enter sensitive data in prompts, keywords, notes, the strategy dialogue or support requests. It does not have pages monitored whose purpose is the publication of sensitive data of individual persons. It does not enter personal data in keywords, nor in prompts for restricted AI assistants (A.4 para. 6). These obligations are contractual rules, not a technical block.

6. **Notices in RankScan:** When prompts and keywords are entered, in the strategy dialogue, for notes and in the support form, RankScan points out the obligation under para. 5. For restricted AI assistants, RankScan points to A.4 para. 6 at the time of selection and when prompts are entered. There is no automatic detection of sensitive data. RankScan also does not automatically detect personal data in prompts or keywords.

5. Nature of the Processing

Collection (crawl of public web pages, retrieval from Search Console and Google Analytics 4, queries to search services and AI assistants), storage, analysis, summarising and review with language models, display, provision via Reporting API and MCP server, dispatch to recipients on the Customer's instruction, deletion.

6. Purposes

Klarplan AG processes Customer Data only for the following purposes:

1. monitoring the technical health, search visibility and AI visibility of the Customer's websites, including in comparison with its competitors
2. set-up in the strategy dialogue and suggestions for prompts, competitors and meta descriptions
3. derivation of measures, summaries, reports, weekly report, shared reports, delegated measures and notifications
4. handling of the Customer's support requests, including triage by a language model
5. provision via the Reporting API and the MCP server
6. operations and security: backups, error analysis and testing of new versions in the test environment (Annex III)
7. quality assurance of measures: a language model reviews samples of derived measures for accuracy in order to improve RankScan's review rules. Insofar as this has effect beyond the individual Customer Account, the evaluation is carried out exclusively on data anonymised beforehand, without reference to persons or Customers.

Purpose limitation. Klarplan AG uses Customer Data only for purposes 1 to 7 and, except for purpose 7, only for the respective Customer. It does not use them for its own advertising, does not sell them, does not train its own AI models with them and discloses them only to sub-processors under Annex IV and to recipients on the Customer's instruction. The authorisation in the GTC to use aggregated, anonymised data covers Customer Data only insofar as they have been anonymised beforehand in such a way that neither a link to a natural person nor an inference about the Customer is possible. Whether a sub-processor uses data for training is stated in Annex IV.

7. Duration of the Processing

For the term of this Agreement (A.2 para. 3). Within the term, the following retention periods apply:

Data	Period
Search and AI visibility results	all runs for 90 days, thereafter one run per month up to 365 days

Data	Period
Website health runs per Plan (all runs / one run per month)	Starter 30/180, Pro 60/365, Enterprise 90/730 days, without a Plan 14/30 days
Raw crawl data (page content)	14 days, thereafter aggregated values only
Failed crawl runs	30 days
Working data of a crawl (link and job queues)	until the end of the run; if aborted, at most two hours longer
Aggregated values (daily values, scores, trends per topic)	25 months
Search Console metrics per page	180 days
Search Console queries per page	replaced at each update, without history
All Search Console data of a website	deleted immediately when Search Console is disconnected
Daily totals from Google Analytics 4 per page and source	365 days
All Google Analytics 4 data of a website	deleted immediately when Google Analytics 4 is disconnected
Resolved technical health findings	180 days
Reviews of pages cited in AI answers	30 days after the last review
Shared reports	30 days from creation
Links for delegated measures	valid for 90 days; content until deletion of the website or the Customer Account
Discarded and failed strategy dialogues	30 days
Export of the Customer Account	7 days, deletion at the latest on the following day
Results of the review of measures	until deletion of the Customer Account
Support requests and screenshots	until deletion on instruction (A.10 para. 5) or deletion of the Customer Account
Team Members, open invitations, contacts, recipients	until removal by the Customer or deletion of the Customer Account
Expired team invitations	30 days after expiry
Customer Account without a Plan (Dormant Period)	12 months, Trial Account 3 months; deletion no earlier than 30 days after the reminder (A.9 para. 2)

8. Processing by Sub-processors

Subject matter, nature and duration are set out per sub-processor in Annex IV. The duration is at most the term of this Agreement. At the sub-processor, the periods in Annex IV apply in addition.

ANNEX III

Technical and Organisational Measures

Including the measures to ensure the security of the data (re Clauses 7.4, 8 and 9).

Encryption and pseudonymisation

- **Transport:** All connections to the application use HTTPS. The TLS connection terminates at Cloudflare (Annex IV no. 10) and is re-encrypted from there to the server. The session cookie is valid only over HTTPS and is encrypted.
- **Secrets:** Search Console and Google Analytics 4 OAuth tokens are stored encrypted in the database. RankScan stores API tokens only as a hash.
- **Storage:** The database (Amazon Lightsail managed database) is encrypted. Lightsail encrypts data at rest automatically. The application server (Amazon Lightsail) stores logs, profile pictures, screenshots of support requests, exports and the test environment database on encrypted volumes (storage volumes with AWS-managed encryption).
- RankScan stores passwords only as a hash.

Confidentiality, integrity, availability, resilience

- **Tenant separation:** Every table containing Customer Data carries the identifier of the Customer Account. Access without a set tenant aborts with an error. Composite foreign keys prevent data in the wrong Customer Account.
- Every background job sets the tenant explicitly before reading or writing data.
- Rate limiting for login, registration, password reset, Reporting API and MCP server.

Recovery after incidents

- Database as an Amazon Lightsail managed database with automatic backups. Retention 7 days, point-in-time recovery within this period. In addition, Klarplan AG backs up the database every night, encrypted, in Amazon S3. These backups are deleted at the latest 35 days after their creation. Manual snapshots are deleted at the latest 30 days after their creation. The backups are located in Frankfurt (eu-central-1). There are no copies in other regions.
- The application server is backed up automatically every day (Lightsail snapshots). The seven most recent are kept. Manual snapshots are deleted at the latest 30 days after their creation.

Review of effectiveness

- Every code change passes automated tests and static analysis before going live.
- **Test environment:** It runs on the application server with its own database. It uses a copy of production. User, account, contact and support data as well as free text from set-up, comments and notes are pseudonymised; usage data and credentials are deleted. Content data such as page content, keywords, prompts, competitors and AI answers remain unchanged. Only Superadmins can log in. Scans there are started only by Superadmins manually, for tests. In doing so, the test environment calls the providers under Annex IV. The copy is replaced at each refresh, at least every 30 days; after a deletion on request, within 10 working days at the latest. The restrictions under A.9 para. 7.3 also apply to tests and provider calls.

- Klarplan AG reviews these measures at least annually and after significant changes to infrastructure or providers.

User identification and authorisation

- Login with e-mail and password. The connection to Google serves only to access Search Console and Google Analytics 4. RankScan requests only read access for Google Analytics 4.
- Roles in the Customer Account: Owner, Admin and Member. Only Admins trigger paid scans, manage the team and delete websites. Only the Owner deletes the Customer Account.
- Access to the Reporting API and MCP server only with a token of the Customer Account. An Admin creates and revokes it. A token from the application is read-only and valid until revoked. It also ends when its creator leaves the Customer Account or is no longer an Admin. Write and delete rights for the MCP server are granted only by Klarplan AG.

Access by Klarplan AG personnel

- Only a few Superadmins have access to Customer Data, and only insofar as operations and support require it.
- When a Superadmin switches into a Customer Account, they have the rights of an Admin there. Every switch writes an entry to the audit log.
- When a Superadmin logs in on behalf of a user, the following actions are blocked: modifying or deleting the profile, creating API tokens, sending invitations, creating or answering support requests, and deleting the Customer Account.
- Superadmin access to RankScan requires a second factor (TOTP). Account switches, including via link, and login on behalf of a user require a verification no older than 15 minutes.
- Exports are created only by a Superadmin on the server, stating a reason in the audit log.
- Administrative AWS access requires MFA.
- All persons with access to Customer Data are contractually bound to confidentiality.

Protection in transit

- HTTPS for the application, Reporting API, MCP server and all calls to sub-processors.
- Only the data required for the respective task are sent to language models and search services. For the language models, Annex IV names them per provider.
- Shared reports and delegated measures are opened via a link with a random token. It is valid for 30 or 90 days respectively.

Protection at rest

- Database and application server at Amazon Web Services, Frankfurt region (eu-central-1).
- The database is not publicly accessible. Only the application server has access.

Physical security

The data centres are operated by Amazon Web Services. Their certifications apply (including ISO 27001, SOC 2). Klarplan AG does not operate its own servers.

Logging

- Application logs with errors and execution times.
- Audit log for Superadmin access to Customer Accounts, exports, deletions, write access via the MCP server, rejected actions, rate-limit hits and failed logins. It contains identifiers, e-mail addresses of the acting persons and IP addresses. For failed logins, only the domain of the entered e-mail address with a shortened hash is recorded instead of the address; for an existing user account, its identifier.
- The logs are not separated by tenant. Only Superadmins have access.
- Retention: application logs 14 days, audit log 365 days.

System configuration

- Server access only via SSH key, through Cloudflare Zero Trust with MFA. Port 22 is closed to the public.
- Security headers for all responses of the application.
- Deployments only from reviewed versions (tag gate).

Internal governance and certification

- Responsible for data protection and IT security: René Häfliger, Member of the Board and Managing Director.
- Security vulnerabilities in dependencies are continuously checked and remedied.
- Klarplan AG holds no certification of its own.

Data minimisation and data quality

- RankScan crawls only public pages and respects robots.txt.
- Intermediate results of a crawl are deleted at the end of the run. Raw page data are reduced to aggregated values after 14 days.
- Search Console and Google Analytics 4 provide only aggregated values, no data on individual visitors. From Google Analytics 4, RankScan stores only totals per page, day and source.
- Without a Plan, RankScan starts no new calls to external services for the Customer Account (A.9 para. 2).
- While a Plan is in place, the Customer can itself modify monitored websites, keywords, prompts, competitors and Team Members (A.10 para. 4).

Limited retention, accountability and data portability

- Automatic deletion according to the periods in Annex II, Section 7.
- This Agreement, the list of sub-processors and the audit log serve as evidence.
- Export via the Reporting API and full export of the Customer Account (A.10 paras. 1 to 3).
- **Deletion:** Deleting a Customer Account immediately blocks the account and removes all Team Members. A background job then deletes all websites, scan results, Search Console and Google Analytics 4 data and credentials, support requests and screenshots, exports, usage data and the Customer Account itself. It deletes user accounts without a further Customer Account together with the profile picture. If the job fails, RankScan repeats it, and the Superadmins receive a notification.

- **Disconnecting Google Analytics 4:** If the Customer disconnects Google Analytics 4 for a website, RankScan immediately deletes all Google Analytics 4 data of that website and then the credentials. RankScan then revokes the authorisation at Google, unless the Customer Account holds another Google access (Search Console or Google Analytics 4). The data is deleted in any case.
- Remaining data: A.9 para. 7.

Assistance to the controller (Clauses 8 and 9)

- Data subject requests: A.10 para. 6.
- Rectification and deletion by the Customer: A.10 paras. 4 and 5.
- Deletion of individual support requests on instruction: A.10 para. 5.
- Notification of breaches under Clause 9.2: without undue delay, at the latest 48 hours after Klarplan AG became aware of the breach, by e-mail to the Owner and the Admins of the Customer Account. The maximum period does not permit any delay where earlier notification is possible.
- Contact point for personal data breaches: hello@rankscan.ai.

Measures of the sub-processors

Klarplan AG requires at least the following measures from every sub-processor: processing only to provide the service and on instruction; no training of AI models with Customer Data (unless Annex IV states otherwise); encryption in transit; access only for authorised personnel bound to confidentiality; deletion according to the periods in Annex IV and at the end of the contract; notification of personal data breaches; assistance with data subject requests.

The contracts of nos. 7 (cloro), 8 (Google Workspace), 9 (DataForSEO) and 10 (Cloudflare) in Annex IV contain these points with two limitations. They do not state an express prohibition of training; they limit processing to the provision of the service. cloro states that it excludes training; this is not contractually guaranteed. cloro's contract does not guarantee encryption in transit; Klarplan AG calls cloro only via HTTPS.

ANNEX IV

List of Sub-processors

Agreed list under Clause 7.7(a) (Option 2). As of 2 November 2026. The current version is available at https://rankscan.ai/subprocessors.

The duration of processing is at most the term of this Agreement. "Not specified" means: the provider's contract makes no statement on this. "Retention at the provider" states the periods at the provider; Klarplan AG's periods are set out in Annex II. "Restricted" denotes a restricted AI assistant under A.4 para. 6 or the service through which such an assistant is queried.

01 **Amazon Web Services EMEA SARL**
38 avenue John F. Kennedy, L-1855 Luxembourg

Activity	Database, application server and test environment (Lightsail), backups (S3), e-mail delivery (SES, Frankfurt)
Customer Data	all Customer Data
Place of processing	EU, Frankfurt (eu-central-1)
Retention at the provider	according to Klarplan AG's periods
Training with Customer Data	no
Transfer basis	Processing in the EU; AWS Data Processing Addendum with SCC 2021/914 and Swiss Addendum

02 **OpenAI Ireland Ltd.** NOT RESTRICTED

1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, Ireland

Activity	Strategy dialogue, suggestions, content briefs, e-mail drafts to cited sources, summaries, triage of support requests, AI visibility
Customer Data	Prompts; topics, keywords, region; positioning, brand terms, competitor names; text of up to 6 pages of the Customer's website (up to 3,000 characters each) with page title and headings (up to 1,000 characters); page title for meta description suggestions; for content briefs, excerpts from answers of the AI assistants (up to 800 characters each) and their search queries, URLs and titles of cited pages, path and page title of the selected page (up to 120 characters); for e-mail drafts, name, address and language of the website, URL and type of the cited source and whether the source grants placements for payment, with the detected word from a fixed list (for example "Sponsored"), without text of the source; in summaries, the content of the measures: keywords with positions, prompts, competitors, URLs and titles of cited pages, Search Console metrics per page (URL, clicks, impressions, click-through rate, position); subject and text of support requests with name and domain of the website, page URL and Plan, without screenshots and without the sender's account details (name, e-mail). Details that the sender writes into the text itself are included.
Place of processing	USA and other countries of OpenAI's sub-processors, without data residency in Europe
Retention at the provider	up to 30 days (abuse monitoring)
Training with Customer Data	no
Transfer basis	The contracting party for customers domiciled in Switzerland is OpenAI Ireland Ltd.; Ireland provides adequate protection under Annex 1 DPO. Data under EEA and Swiss law are processed by OpenAI Ireland Limited. OpenAI bases onward transfers outside the EEA and Switzerland, for example to OpenAI OpCo, LLC, on SCC 2021/914 (DPA of 1 January 2026, para. 4.1). The DPA does not provide for an adaptation of the SCC for Switzerland in this respect. OpenAI OpCo, LLC is not certified under the Data Privacy Framework.

03 Google Cloud EMEA Limited NOT RESTRICTED

Velasco, Clanwilliam Place, Dublin 2, Ireland

Activity	Gemini API (paid tier): AI visibility with Google Search, review of measures, review of own mentions
Customer Data	Prompts; excerpts from AI answers; business context (brand, domain, topics, keywords, region); name and domain of the website; text of the measure with the most frequent queries, impressions, clicks and position per page from Search Console; result of the measurement review with the page title from the last retrieval (up to 120 characters)
Place of processing	not specified
Retention at the provider	55 days (abuse monitoring); with Google Search 30 days, cannot be disabled
Training with Customer Data	no
Transfer basis	Data Processing Addendum for Products Where Google is a Data Processor with SCC 2021/914; the DPA also covers data under the FADP. Google LLC is certified under the EU-U.S. and the Swiss-U.S. Data Privacy Framework.

04 Groq UK Limited NOT APPLICABLE

3 Hammersmith Grove, London W6 0ND, United Kingdom

Activity	Evaluation of AI answers: brands, relevance, suitability of cited pages. Groq receives no AI visibility prompts; it evaluates answers.
Customer Data	Answer texts; business context (brand or website name, domain, topics, up to 60 keywords, region); names of brands and competitors; URL, title and up to 4,000 characters of text of third-party pages cited in an AI answer
Place of processing	USA (Google Cloud)
Retention at the provider	none by default; logs in the event of malfunction or abuse for up to 30 days
Training with Customer Data	no
Transfer basis	Groq Data Processing Addendum with SCC 2021/914 (Modules 2 and 3) and adaptation for Switzerland

05 Anthropic Ireland, Limited NOT RESTRICTED

6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland

Activity	AI visibility, only if selected by the Customer
Customer Data	Prompts
Place of processing	worldwide at the provider's discretion
Retention at the provider	30 days; up to 2 years in the event of a violation of the usage policies
Training with Customer Data	no
Transfer basis	Anthropic Data Processing Addendum with SCC 2021/914 (Modules 2 and 3) and Swiss Addendum. Anthropic, PBC (USA) is not certified under the Data Privacy Framework.

06 Perplexity AI, Inc. RESTRICTED

115 Sansome Street, Suite 900, San Francisco, CA 94104, USA

Activity	AI visibility, only if selected by the Customer
Customer Data	Prompts
Place of processing	USA. Perplexity and all of its sub-processors are located in the USA.
Retention at the provider	Personal data in inputs until deletion by the customer, at the latest 30 days after the end of the service (DPA Annex 1). Separate rules may apply to individual services.
Training with Customer Data	no (DPA §5)
Transfer basis	Perplexity Data Processing Addendum (version of 13 August 2026) with SCC 2021/914 (Modules 2 and 3) for data under EU and UK law. The DPA does not cover data under the FADP. Perplexity AI, Inc. is not certified under the Data Privacy Framework. Klarplan AG has prepared a transfer impact assessment and reviews it at least annually.

07 Cloro Incorporation Ltd. RESTRICTED

168 Triq San Kristofru, Valletta VLT 1467, Malta

Activity	Querying Microsoft Copilot, only if selected by the Customer
Customer Data	Prompts, country code of the website
Place of processing	USA (application, database and backups at DigitalOcean) and Germany (query at Hetzner). The request to Copilot is sent from the website's country. Further sub-processors of cloro with purpose and location: https://cloro.dev/our-commitment-to-security/ (section "Subprocessors").
Retention at the provider	Synchronous requests and results are not stored after the response; asynchronous jobs and results for about 24 hours; telemetry including the text of the prompts for 6 months; application logs 7 days; backups 7 to 14 days; deletion on request within 30 days. These periods are stated by cloro; they are not contractually guaranteed.
Training with Customer Data	no according to cloro, not contractually guaranteed; the Terms (§6.2) permit only aggregated, de-identified use. Microsoft may use the prompts to improve Copilot (A.4 para. 5).
Transfer basis	Disclosure to cloro (Malta): adequate protection under Art. 16(1) FADP and Annex 1 DPO; within the EU no transfer under Chapter V GDPR. Onward transfer to DigitalOcean, LLC (USA): DigitalOcean is certified under the EU-U.S. and the Swiss-U.S. Data Privacy Framework. In addition, the cloro Data Protection Agreement with SCC 2021/914 (Module 2) applies; para. 6(a) places transfers from Switzerland under the SCC; the DPA contains no adaptation to the FADP and the FDPIC. For Better Stack (logs; Germany and USA) and Snapshooter (backups; USA), the contract between cloro and the service applies. Klarplan AG does not know this contract. cloro is liable for both under DPA §5(c). The onward transfer to Microsoft Copilot takes place on the Customer's instruction (A.4 para. 5; clause 8.8 of the cloro Data Protection Agreement).

08 Google Cloud EMEA Limited: Google Workspace

Velasco, Clanwilliam Place, Dublin 2, Ireland

Activity	Mailbox hello@rankscan.ai: support, instructions, internal notification of support requests
Customer Data	Content of the Customer's e-mails; excerpts from support requests
Place of processing	not specified
Retention at the provider	according to Klarplan AG's periods
Training with Customer Data	not specified
Transfer basis	Google Cloud Data Processing Addendum, accepted for the rankscan.ai account

09 DataForSEO OÜ

Vesivärava tn 50-201, 10152 Tallinn, Estonia, registration number 14502291

Activity	Retrieval of search results (SERP), keyword metrics and search visibility
Customer Data	Keywords, domains, URLs, language and country settings (personal data only insofar as search results contain them)
Place of processing	EU (Estonia, Germany at Hetzner) and USA (Google Cloud, Microsoft Azure)
Retention at the provider	Job data temporarily cached after retrieval; logs according to the provider's periods
Training with Customer Data	no
Transfer basis	Disclosure to DataForSEO OÜ (Estonia): adequate protection under Art. 16(1) FADP and Annex 1 DPO; within the EU no transfer under Chapter V GDPR. Onward transfer to sub-processors in the USA: DataForSEO Data Processing Agreement (part of the Privacy Policy) with Standard Contractual Clauses (SCC).

10 Cloudflare, Inc.

101 Townsend Street, San Francisco, CA 94107, USA

Activity	Reverse proxy, DDoS protection and web application firewall for the application, reporting API, MCP server and test environment; server access (Zero Trust)
Customer Data	all data in the traffic with the application, reporting API, MCP server and test environment, including users' IP addresses and browser data. The TLS connection terminates at Cloudflare (Annex III).
Place of processing	worldwide, in the Cloudflare data centre closest to the user; also outside the EEA and Switzerland (DPA para. 6.1)
Retention at the provider	not specified; the DPA limits processing to the term of the contract with Cloudflare or until it is no longer necessary for the service (Annex 1)
Training with Customer Data	not specified; the DPA limits processing to the provision of the service (para. 3.1(a))
Transfer basis	Cloudflare Data Processing Addendum (version 6.4 of 3 April 2026), part of the Self-Serve Subscription Agreement. Cloudflare, Inc. is certified under the EU-U.S. and the Swiss-U.S. Data Privacy Framework. If the certification lapses, the SCC 2021/914 (Modules 2 and 3) with the adaptation for Switzerland apply under DPA para. 6.2.

Default selection of AI assistants. Without a selection of its own by the Customer, the prompts of a new website are sent to OpenAI and Gemini. Anthropic, Perplexity and cloro receive prompts only if the Customer selects them. Restricted AI assistants (A.4 para. 6) are never part of the default selection.

Services without Processing on Behalf

RankScan uses the following services. They are not sub-processors.

Service	Classification	Reasoning
Google LLC: Search Console API	independent controller; data source of the Customer	The Customer connects its Search Console. Google provides data from its own search under the Google APIs Terms with controller-to-controller terms. RankScan sends only the credentials and page URLs.
Google LLC: Chrome UX Report API	service without personal data	RankScan sends only page URLs and receives aggregated loading times.
Google LLC: Favicon service (S2)	service without personal data in the specific use	RankScan queries the service only if a website does not provide a favicon itself. The server sends only the domain name, no IP address or browser data of users.
Wikimedia Foundation, Inc.: Wikidata	service without personal data in the specific use	RankScan sends only the domain of the website as the search term.
Serper (Serper.dev)	service without personal data in the specific use	RankScan sends Serper exclusively topic-related search terms (keywords) and the country and language code, without domain, account, user or IP data of the Customer, in order to retrieve public Google search results. The entry of personal data in keywords is excluded under Annex II, Section 4 para. 5.
Third-party websites	no recipient	RankScan retrieves public pages, including favicons of competitors, and sends only the request.
Google Tag Manager, Google Analytics 4, Google Ads, OpenAI pixel in the application	area of responsibility of Klarplan AG; only with consent	Measurement of registration and subscription in accordance with the Privacy Policy.
Stripe, Mautic (self-hosted)	area of responsibility of Klarplan AG	Billing and own e-mails.
Microsoft (Copilot)	recipient on the Customer's instruction (A.4 para. 5); independent controller without a contract with Klarplan AG	cloro submits the prompts to the consumer interface of Microsoft Copilot, only if selected by the Customer. Microsoft processes them under its own terms and may use them to improve Copilot.
Services connected by the Customer, for example Looker Studio or an MCP client	recipient on the Customer's instruction	The Customer connects them itself. They are not sub-processors of Klarplan AG.