

Data Processing Agreement (Art. 28 GDPR)

Version 1.3, 6 October 2026

This Data Processing Agreement ("DPA") is entered into between the Customer identified in Annex I (the "controller") and pulse Energy GmbH, d/b/a Sitefire (the "processor"). It consists of the Standard Contractual Clauses adopted by the European Commission in Commission Implementing Decision (EU) 2021/915 of 4 June 2021 (Sections I to III below, reproduced without modification, with the options selected and the Annexes completed), the Supplementary Terms, and Annexes I to IV.

Standard Contractual Clauses

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 – 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 access 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.

Supplementary Terms

These Supplementary Terms are additional clauses within the meaning of Clause 2(b). They do not modify the Clauses. If a Supplementary Term contradicts the Clauses, the Clauses prevail (Clause 4).

In these Supplementary Terms, "Sitefire" means the processor, "Customer" means the controller, and "Customer Personal Data" means the personal data described in Annex II that Sitefire processes on behalf of the Customer.

S.1 Relation to the main agreement

(a) The main agreement between the Parties is the Sitefire General Terms and Conditions (AGB) published at <https://sitefire.ai/terms>, together with any order form or plan the Customer selects (the "Main Agreement"). § 7 of the AGB incorporates this DPA by reference.

(b) This DPA applies to the extent that Sitefire processes Customer Personal Data on behalf of the Customer in the course of providing the services under the Main Agreement.

(c) In the event of a contradiction between this DPA and the Main Agreement with respect to the processing of Customer Personal Data, this DPA prevails.

(d) The Customer's documented instructions under Clause 7.1 are given by this DPA (including Annex II), by the Main Agreement, and by the Customer's configuration and use of the service. The Customer may give further documented instructions in writing, including by email to privacy@sitefire.ai.

S.2 No use of Customer Personal Data for AI training or for Sitefire's own purposes

(a) Sitefire does not use Customer Personal Data to train or improve artificial intelligence models, and does not use Customer Personal Data for its own purposes.

(b) Anonymised and aggregated statistics under § 5 of the AGB ("Aggregated Statistics") do not relate to an identified or identifiable natural person and therefore fall outside the scope of this DPA.

(c) The Customer may opt out of the use of Aggregated Statistics for improving AI models by sending an email to privacy@sitefire.ai.

S.3 International transfers

(a) Where a sub-processor listed in Annex IV processes Customer Personal Data outside the European Economic Area, the Customer instructs Sitefire, within the meaning of Clause 7.8(a), to carry out that transfer on one of the following bases under Chapter V of Regulation (EU) 2016/679:

1. for a sub-processor in the United States that is certified under the EU-U.S. Data Privacy Framework, the adequacy decision of the European Commission of 10 July 2023 (Commission Implementing Decision (EU) 2023/1795); or
2. otherwise, the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Three (processor to processor), concluded between Sitefire and the sub-processor in accordance with Clause 7.8(b).

(b) Where a sub-processor is established in the European Economic Area and itself transfers Customer Personal Data to a third country, that sub-processor ensures compliance with Chapter V of Regulation (EU) 2016/679 under its contract with Sitefire (Clause 7.7(b)).

(c) Annex IV states the transfer basis for each sub-processor.

S.4 Liability and governing law

(a) The liability of the Parties under or in connection with this DPA is governed by the liability provisions of the Main Agreement (currently § 6 of the AGB).

(b) This DPA is governed by the law that governs the Main Agreement, and the place of jurisdiction of the Main Agreement applies (currently § 8 of the AGB: German law, exclusive venue Munich, Germany).

S.5 Time limit for the notification of a personal data breach

(a) Sitefire notifies the Customer of a personal data breach concerning Customer Personal Data (Clause 9.2) without undue delay, at the latest within 48 hours of becoming aware of it.

(b) Sitefire sends the notification by email to the contact person named in Annex I. Where not all information listed in Clause 9.2 is available within 48 hours, Sitefire sends the information then available and sends further information without undue delay as it becomes available.

S.6 List of sub-processors and notice of changes

(a) Sitefire publishes the current list of sub-processors at <https://sitefire.ai/subprocessors>. On the date of this DPA, that list is the list in Annex IV.

(b) Sitefire notifies the Customer of any intended addition or replacement of a sub-processor (Clause 7.7(a)) by email to the contact person named in Annex I, at least 30 days in advance.

S.7 Amendments

(a) Changes to this DPA require the agreement of both Parties in writing. Email is sufficient.

(b) The following changes do not require the agreement of the Customer:

1. Changes to the list of sub-processors in Annex IV. These follow Clause 7.7(a) and Supplementary Term S.6.
2. Updates to the technical and organisational measures in Annex III that do not reduce the overall level of protection of Customer Personal Data. Sitefire informs the Customer of these updates by email to the contact person named in Annex I.

(c) The procedure for changes to the AGB (currently § 11 of the AGB) does not apply to this DPA.

ANNEX I – List of parties

Controller(s)

Name: The Customer identified in the order form or in the Customer's Sitefire account: _____

Address: _____

Contact person's name, position and contact details: _____

Data protection officer (where applicable): _____ (name and contact details, or "not appointed")

Activities relevant to the processing under these Clauses: use of the Sitefire services as described in Annex II.

Role: controller

Signature and accession date: _____ / Date: _____

Processor(s)

Name: pulse Energy GmbH, doing business as "Sitefire"

Address: Kellerstr. 30, 81667 München, Germany

Commercial register: Amtsgericht München, HRB 299092

VAT ID: DE452862576

Managing directors: Jochen Madler, Vincent Jeltsch

Contact person's name, position and contact details: Vincent Jeltsch, Managing Director (Geschäftsführer), privacy@sitefire.ai

Data protection officer (where applicable): not appointed. A data protection officer is not required under § 38 BDSG.

Activities relevant to the processing under these Clauses: provision of the Sitefire AI-visibility analytics platform as described in Annex II.

Role: processor

Signature and accession date: _____ / Date: _____

ANNEX II – Description of the processing

Subject matter

Provision of the Sitefire AI-visibility analytics platform to the Customer: monitoring of brand mentions and citations in answers of AI systems, analytics connectors, AI features and agents (including tools that the Customer connects), content creation, and customer support.

Categories of data subjects whose personal data is processed

1. The Customer's authorised users of the Sitefire platform (employees and contractors of the Customer).
2. Persons who are named in content that the Customer provides to Sitefire, or in content that Sitefire retrieves from a tool that the Customer connects.
3. Visitors of the Customer's websites, only to the extent that analytics data from a connected analytics source relates to them.

Categories of personal data processed

Sitefire processes the data from a connector only when the Customer connects it. The Customer can disconnect a connector at any time.

1. **User account data:** name, business email address, role, login and audit logs (including IP address and user agent).
2. **Content that the Customer enters, uploads or makes available through a connected tool:** brand context, prompts, files, agent instructions, messages that users send to Sitefire agents through Slack or Microsoft Teams, and the data that Sitefire agents read from or write to connected tools (see items 8 to 10). This content can contain names and contact details.
 - Prompts and keywords are business queries. They are not intended to contain personal data.
3. **Support communications:** messages exchanged between the Customer's users and Sitefire support.
4. **Connected analytics data – Google Analytics 4 (GA4),** only when the Customer connects it:
 - Sitefire retrieves aggregated reports only.
 - Dimensions: date, sessionSource, sessionMedium, landingPage (path without URL parameters), hostName.
 - Metrics: sessions, totalUsers, newUsers, engagedSessions, bounceRate, engagementRate, averageSessionDuration, screenPageViews, screenPageViewsPerSession, conversions, sessionConversionRate.
 - The reports are filtered to sessions referred by the following AI platforms: chatgpt.com, chat.openai.com, gemini.google.com, perplexity.ai, claude.ai, you.com, phind.com, copilot.microsoft.com, poe.com.
 - Sitefire does not retrieve IP addresses, user IDs, client IDs, location data or device data from GA4.
 - Access is read-only, with the Viewer role, through a Google service account that Sitefire creates for each Customer.
 - Sitefire treats these aggregated reports as anonymous statistics. They are included in this DPA as a precaution, in case they are considered personal data.

5. **Connected analytics data – Google Search Console**, only when the Customer connects it:
 - Dimensions: date and page.
 - Metrics: clicks, impressions, ctr, position.
 - Sitefire does not store search queries.
 - These are aggregated statistics. They are included in this DPA as a precaution, in case they are considered personal data.
6. **Connected analytics data – Bing Webmaster Tools**, only when the Customer connects it: aggregated statistics of the Customer's website (traffic, ranking, page, search query and crawl statistics, and sitemaps).
7. **Connected analytics data – CDN logs (Cloudflare, Amazon CloudFront)**, only when the Customer connects them: requests from AI crawlers, identified by their user agent. Sitefire uses the date, page path, host, HTTP status, content type and user agent of these requests. Sitefire does not use IP addresses from CDN logs.
8. **Google Drive**, only when the Customer connects it: Sitefire creates export files in the Customer's Google Drive. Sitefire uses the access scope `drive.file`, which gives access only to the files that Sitefire creates. Sitefire also receives the email address of the Google account that connects Google Drive.
9. **CMS connectors (Webflow, Framer, Sanity, Hygraph, dotCMS)**, only when the Customer connects them: access credentials and the structure of the Customer's CMS. Sitefire publishes content to the CMS at the Customer's request.
10. **Tools connected through Composio**, for example Slack, Microsoft Teams, Intercom, Granola, Notion and Confluence, only when the Customer connects them: OAuth connection data, and the data that a Sitefire agent reads from or writes to the tool when it carries out a task. This data can include messages, documents, meeting notes and support conversations, and the names and contact details of the persons in them.

Sensitive data processed (if applicable) and applied restrictions or safeguards

The processing of special categories of personal data (Art. 9 GDPR) or of personal data relating to criminal convictions and offences (Art. 10 GDPR) is not intended. The service is not designed for such data.

Nature of the processing

Collection through connectors, storage, retrieval, analysis, transmission of tracked prompts to AI systems to retrieve their answers, transmission to AI model providers when users run AI features, transmission to connected tools when agents carry out tasks, and deletion.

Purpose(s) for which the personal data is processed on behalf of the controller

1. Provision of the contracted Sitefire services and of customer support.
2. Security of the service and troubleshooting.

Duration of the processing

1. Sitefire processes Customer Personal Data for the term of the Customer's subscription. No maximum retention period applies during the term.
2. Sitefire deletes Customer Personal Data within 3 months after the end of the subscription. This period allows the Customer to reactivate the subscription without loss of data.
3. On request, Sitefire confirms the deletion to the Customer.
4. Backups: Sitefire makes daily backups of the Supabase and ClickHouse databases and keeps each backup for 7 days. Data that Sitefire deletes is therefore removed from all backups within 7 days.
5. AI traces in PostHog: PostHog deletes the content of AI trace events (inputs, outputs and tool data) after 30 days. The metadata of these events, without content, is kept according to PostHog's retention period. Error messages of failed AI calls (up to 2,000 characters) are part of the metadata.

6. Correction, deletion and export: the Customer can request the correction, deletion or export of Customer Personal Data by email to privacy@sitefire.ai. Sitefire carries out the request within 30 days. Exports are in CSV or JSON format.

For processing by (sub-)processors: subject matter, nature and duration

The sub-processors, the subject matter of their processing (purpose), the categories of data, the location of processing and the transfer basis are listed in Annex IV. The nature of their processing is as described above, limited to the purpose stated for each sub-processor in Annex IV. The duration of their processing is the duration stated above, limited to the period for which Sitefire uses the sub-processor.

ANNEX III – Technical and organisational measures including technical and organisational measures to ensure the security of the data

Sitefire holds no security certifications (for example, no ISO/IEC 27001 certification and no SOC 2 report).

1. Measures of pseudonymisation and encryption of personal data

1. All data in transit between users, the Sitefire web application, Sitefire's backend services and sub-processors is encrypted with TLS.
2. Data at rest is encrypted by the hosting providers with provider-managed encryption (Supabase, Vercel, ClickHouse).
3. The private key of each Customer's Google service account is stored in Supabase Vault (encrypted secret storage) and can be read only by the server role.
4. All staff laptops use full-disk encryption.
5. Pseudonymisation: Sitefire does not pseudonymise Customer Personal Data. Protection relies on encryption, access control and tenant separation.

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

1. Multi-tenant isolation: every data record is assigned to a Customer by its `company_id`. Postgres row-level security enforces this isolation in the database. A custom JWT access-token hook adds the user's `company_id` and role to the access token, and the row-level security policies use these claims.
2. Role-based access control in the application, with the roles Admin and Viewer.
3. The services run on managed cloud infrastructure of the sub-processors listed in Annex IV.
4. Availability: Sitefire gives no contractual availability target. Sitefire monitors its services with Vercel, Supabase and PostHog. Alerts go to Sitefire's Slack workspace.

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

1. Backups: daily backups of the Supabase and ClickHouse databases, kept for 7 days.
2. Incident response: Sitefire has a written incident procedure. The incident owner is Vincent Jeltsch (Managing Director). The backup owner is Jochen Madler (Managing Director). Sitefire records every incident in an incident log.

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

1. Every code change goes through a pull request. Automated checks (lint, unit tests, backend tests, type checks and database tests) run on every pull request before the change is merged.
2. Database schema changes are deployed only through the integration between the source code repository and Supabase. They are not applied to the production database directly.
3. Sitefire reviews these technical and organisational measures and its written security policy once a year.
4. Security testing: Sitefire did an internal security review in March 2026 and fixed all critical and high findings. Sitefire has not had an external penetration test.

5. Measures for user identification and authorisation

1. Users authenticate with a one-time code sent by email, with a password, or with Google sign-in.
2. Authorisation in the application is role-based (Admin and Viewer) and limited to the user's own Customer account (see section 2).
3. Multi-factor authentication is enabled on all staff accounts with access to customer data.
4. Staff access: Sitefire gives staff access to Customer Personal Data according to their role, and only as far as their role requires. Engineers get access to production data. Go-to-market staff get access to the Customer Personal Data that their work requires. At present, only the two managing directors have access.
5. Every person signs a confidentiality undertaking before they get access (section 11).
6. Sitefire removes a person's access within 14 days after their contract ends.

6. Measures for the protection of data during transmission

1. TLS encryption for all connections (see section 1).
2. HTTP Strict Transport Security (HSTS) and further security headers on the Sitefire web application.
3. Access to Google Analytics uses the read-only OAuth scope `analytics.readonly` and the GA4 Viewer role.

7. Measures for the protection of data during storage

1. Provider-managed encryption at rest (see section 1).
2. Secrets (such as service account keys) are stored in Supabase Vault and are readable only by the server role.
3. Hosting region: Frankfurt am Main, Germany, for Vercel functions (region fra1) and the Supabase database (region eu-central-1). ClickHouse and PostHog are used in their EU regions. Vercel Blob file storage is in Washington, D.C., USA (region iad1) until Sitefire moves it to Frankfurt.

8. Measures for ensuring physical security of locations at which personal data are processed

1. Customer Personal Data is stored with the hosting sub-processors listed in Annex IV. The physical security of their data centres is provided by these sub-processors under their contracts with Sitefire.
2. All staff laptops use full-disk encryption.
3. Staff keep extracts of production data on their devices only for support or debugging. They delete the extracts when the task ends.

9. Measures for ensuring events logging

1. Operational logs are collected centrally in Vercel, Supabase and PostHog.
2. Login and audit logs of user activity, including IP address and user agent, are kept.

3. Log retention: operational logs are kept for up to 7 days.

10. Measures for ensuring system configuration, including default configuration

1. Production and test environments are separate. Changes are tested in separate preview environments before they reach production.
2. Security headers and HSTS are configured by default on the web application.
3. New connections to Google Analytics are configured with read-only access by default (section 6).

11. Measures for internal IT and IT security governance and management

1. The managing directors of pulse Energy GmbH are responsible for data protection and information security.
2. Sitefire has a written security and data protection policy. The managing directors review it once a year.
3. Every person with access to Customer Personal Data signs a written confidentiality undertaking ("Verpflichtung auf Vertraulichkeit und Datenschutz") before they get access (Clause 7.4(b)).

12. Measures for certification/assurance of processes and products

Sitefire holds no certifications. In accordance with Clause 7.6, Sitefire provides the information necessary to demonstrate compliance and permits and contributes to audits.

13. Measures for ensuring data minimisation

1. From Google Analytics 4, Sitefire retrieves only aggregated reports with the dimensions and metrics listed in Annex II. Landing pages are stored as paths without URL parameters. Sitefire does not retrieve IP addresses, user IDs, client IDs, location data or device data.
2. GA4 reports are filtered to sessions referred by the AI platforms listed in Annex II.
3. From Google Search Console, Sitefire stores only the dimensions and metrics listed in Annex II. Sitefire does not store search queries.
4. From CDN logs, Sitefire uses only requests from AI crawlers and does not use IP addresses.
5. Access to analytics connectors is read-only. Google Drive access is limited to the files that Sitefire creates.
6. Each connector processes data only when the Customer connects it.

14. Measures for ensuring data quality

1. Connected analytics data is retrieved directly from the source system through its API.
2. The Customer can request the correction of Customer Personal Data by email to privacy@sitefire.ai. Sitefire corrects the data within 30 days.

15. Measures for ensuring limited data retention

1. Customer Personal Data is deleted within 3 months after the end of the subscription (Annex II).
2. Backups are kept for 7 days. Deleted data is removed from all backups within 7 days.
3. PostHog deletes the content of AI trace events after 30 days (Annex II).

16. Measures for ensuring accountability

1. This DPA and the list of sub-processors in Annex IV are kept up to date.
2. Each sub-processor is engaged under a written data processing agreement (Clause 7.7(b)).
3. Sitefire keeps a record of processing activities as processor (Art. 30(2) GDPR).

17. Measures for allowing data portability and ensuring erasure

1. Deletion of Customer Personal Data after the end of the subscription as described in Annex II, with confirmation of deletion on request.
2. Return or export of Customer Personal Data at the Customer's choice (Clause 10(d)): on request by email to privacy@sitefire.ai, Sitefire exports the data in CSV or JSON format within 30 days.

Measures for transfers to (sub-)processors

Sitefire engages sub-processors only under a contract that imposes, in substance, the same data protection obligations as this DPA (Clause 7.7(b)). Sub-processors that process Customer Personal Data outside the EEA do so on the transfer basis stated in Annex IV.

Specific technical and organisational measures to assist the controller

1. **Data subject requests (Clause 8):** Sitefire forwards any request from a data subject that it receives to the Customer without undue delay and does not respond to the request unless the Customer authorises it. The contact point for the Customer is privacy@sitefire.ai. The Customer can request access to, correction, export (CSV or JSON) or deletion of personal data by email to privacy@sitefire.ai. Sitefire carries out the request within 30 days.
2. **Personal data breaches (Clause 9):** Sitefire notifies the Customer without undue delay, at the latest within 48 hours of becoming aware of a personal data breach (Supplementary Term S.5), by email to the contact person named in Annex I. The notification contains the information listed in Clause 9.2. The contact point at Sitefire is privacy@sitefire.ai.
3. **Data protection impact assessments and prior consultation (Clause 8(c)):** on request, Sitefire provides the Customer with the information about the processing that is available to Sitefire, including this Annex III and Annex IV.

ANNEX IV – List of sub-processors

The controller has authorised the use of the following sub-processors (Clause 7.7(a), general written authorisation; this Annex is the agreed list). The current list is published at <https://sitefire.ai/subprocessors> (Supplementary Term S.6).

Data categories (see Annex II): **A** = user account data; **B** = content that the Customer enters, uploads or makes available through a connected tool; **C** = support communications; **D** = connected analytics data.

Transfer status: "DPF certified" means that the entity is listed as active on the EU-U.S. Data Privacy Framework List (www.dataprivacyframework.gov/list), checked 2026-10-06.

Part A – Sub-processors

#	Sub-processor	Legal entity and address	Purpose	Data categories	Location of processing	Transfer mechanism
1	Vercel	Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting of the web application; serverless functions; workflows; AI Gateway (routing of requests to AI model providers); Blob file storage; Sandbox (isolated execution of agent tasks)	A, B, C, D	Functions: Frankfurt, Germany (region fra1). Blob: Washington, D.C., USA (region iad1), until Sitefire moves it to Frankfurt. Sandbox: region not configurable today; processing may occur outside the EU. Sitefire moves it to the EU as soon as Vercel supports this. Workflows and AI Gateway: region not fixed by Vercel. Vercel states that its primary processing facilities are in the USA.	EU-U.S. DPF: DPF certified (checked 2026-10-06)
2	Supabase	Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Primary database, user authentication, secret storage (Vault)	A, B, C, D	Frankfurt, Germany (AWS region eu-central-1)	Not found on DPF list (Singapore entity) → SCCs 2021/914, Module Three, as incorporated in the Supabase DPA
3	ClickHouse	ClickHouse, Inc., c/o Goodwin Procter LLP, 601 Marshall St, Redwood City, CA 94063, USA	Analytics database	B, D (prompts, AI answers and analytics data; no account data)	EU region of ClickHouse Cloud. ClickHouse states that its control plane runs in the USA, Germany and Singapore.	EU-U.S. DPF: DPF certified (checked 2026-10-06)
4	PostHog	PostHog, Inc., 2261 Market Street #4008, San Francisco, CA 94114, USA	Product analytics, error tracking, logs of AI feature calls (AI traces). PostHog deletes the content of AI traces after 30 days. DPA signed 2026-10-06.	A, B (in AI traces)	Frankfurt, Germany (PostHog EU Cloud)	EU-U.S. DPF: DPF certified (checked 2026-10-06)
5	Google Cloud and Google Workspace	Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Google Cloud IAM: creation and management of one Google service account per Customer for read-only access to the Customer's Google Analytics and Google Search Console. Google Workspace (Gmail, Google Drive): email and documents, including support communications with the Customer	A, C, D (service account identifiers and access to the Customer's analytics property; email and support communications)	IAM: Google lists IAM as a service that does not store Customer Data at rest or process Customer Data in use. Google Workspace: Google's global data centres	Entity in the EEA, no transfer by Sitefire. Onward transfers by Google under the SCCs in the Google Cloud Data Processing Addendum.
6	Google Gemini API	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Large language model (Gemini) for AI features; retrieval of AI answers to the Customer's tracked prompts for monitoring	B	No region selection available; Google states that logs may be stored transiently in any country	EU-U.S. DPF: Google LLC DPF certified (checked 2026-10-06)

#	Sub-processor	Legal entity and address	Purpose	Data categories	Location of processing	Transfer mechanism
7	Anthropic	Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	Large language model (Claude, default model) for AI features	B	USA and other countries outside the EEA, as stated by Anthropic	Entity in the EEA, no transfer by Sitefire. Onward transfers by Anthropic under SCCs 2021/914 in the Anthropic DPA. (Anthropic not found on DPF list.)
8	OpenAI	OpenAI Ireland Ltd., 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Large language model for AI features; retrieval of AI answers to the Customer's tracked prompts for monitoring	B	Global (OpenAI default; no EU data residency)	Entity in the EEA, no transfer by Sitefire. Onward transfers by OpenAI under SCCs or adequacy decisions as stated in the OpenAI DPA. (OpenAI not found on DPF list.)
9	Perplexity	Perplexity AI, Inc., 115 Sansome Street Suite 900, San Francisco, CA 94104, USA	Large language model and web search API for AI features; retrieval of AI answers to the Customer's tracked prompts for monitoring	B	USA	EU-U.S. DPF: DPF certified (checked 2026-10-06)
10	Composio	Sampark, Inc. d/b/a Composio, 2 Bryant St., Suite 220, San Francisco, CA 94105, USA	Connector platform: storage of OAuth connections to tools that the Customer connects (for example Slack, Microsoft Teams, Intercom, Granola, Notion, Confluence) and execution of connector actions for agent features. Zero data retention is enabled. DPA accepted 2026-10-06.	A, B (OAuth tokens, connection metadata, data passed through connector actions)	USA (AWS region us-east-1)	Not found on DPF list → SCCs 2021/914, Module Three, as incorporated in the Composio DPA
11	Resend	Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA	Sending of transactional emails (for example sign-in codes and notifications)	A, B (email content)	USA	EU-U.S. DPF: DPF certified (checked 2026-10-06; status "Active – Re-certification under Review")
12	Slack	Slack Technologies Limited, Dublin, Ireland	Internal communication, and shared channels with Customers, including support communications	A, C	Slack's data centres	Entity in the EEA, no transfer by Sitefire. Onward transfers by Slack under the SCCs in the Slack DPA.
13	Cloudflare	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Bot protection (Turnstile) on sign-in, password reset and email verification forms. Cloudflare processes the Turnstile signals as processor to detect bots. Cloudflare states that it also uses these signals as an independent controller to improve Turnstile.	A (IP address, user agent, TLS fingerprint)	Cloudflare global network	EU-U.S. DPF: DPF certified (checked 2026-10-06; status "Active – Re-certification under Review")

Part B – Other service providers (for information; not sub-processors)

The following providers do not process Customer Personal Data on behalf of the Customer. Stripe and Attio process personal data for Sitefire's own purposes, with Sitefire (or the provider) as controller. Firecrawl and DataForSEO receive no Customer Personal Data. Stripe and Attio receive billing and sales contact data only, no Customer content.

Provider	Legal entity and address	Purpose	Role
Stripe	Stripe Payments Europe, Limited, One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland	Payment processing and billing of the Sitefire subscription	Sitefire as controller for its billing data; Stripe states that it acts as processor for some services and as independent controller for others (for example fraud prevention and legal compliance)
Attio	Attio Limited, 42 St John's Square, 2nd Floor, London EC1M 4EA, United Kingdom	Customer relationship management (Sitefire's own sales and customer records)	Sitefire as controller
Firecrawl	SideGuide Technologies, Inc. d/b/a Firecrawl (Delaware corporation), USA	Retrieval of public web pages at URLs that Sitefire or an agent provides, and site searches of the form "site:CUSTOMER-DOMAIN TOPIC"	Not a sub-processor: Firecrawl receives only public URLs, domains and business topics, no Customer Personal Data
DataForSEO	Dataforseo OÜ, Tallinn, Estonia	Keyword and search engine data; retrieval of AI answers (for example ChatGPT, Gemini, Google AI Mode) to tracked prompts	Not a sub-processor: DataForSEO receives keywords, domains and prompts, which are business queries and contain no Customer Personal Data (see Annex II)

Signatures

Controller (Customer)

Company: _____

Name: _____

Position: _____

Place, date: _____

Signature: _____

Processor

pulse Energy GmbH (d/b/a Sitefire)

Name: Vincent Jeltsch

Position: Managing Director (Geschäftsführer)

Place, date: München, _____

Signature: _____