DIVER

Data Processing Agreement

Effective Date: April 19, 2026 · Last Updated: April 19, 2026

Draft — to be reviewed by counsel before relying on it for production EU contracts.

This Data Processing Agreement ("DPA") forms part of the Terms of Service between you ("Customer", the data controller) and Diver, operated by Greenhat Webs ("Diver", the data processor) and applies to the extent that Diver processes Personal Data on Customer's behalf in providing the Service.

Contents

Annexes

1. Parties & Effective Date

This DPA is entered into between the Customer (the "Controller") and Diver, operated by Greenhat Webs (the "Processor"), each a "Party" and together the "Parties". It takes effect on the Effective Date set out above (or, if later, the date the Customer first accepts the Terms of Service) and remains in force for as long as Diver processes Personal Data on the Customer's behalf.

2. Definitions

Capitalised terms not defined herein have the meaning given in the GDPR (Regulation (EU) 2016/679) and the UK GDPR. For the avoidance of doubt:

- **Controller —** the natural or legal person which determines the purposes and means of the Processing of Personal Data.
- **Processor —** the natural or legal person which processes Personal Data on behalf of the Controller.
- **Personal Data —** any information relating to an identified or identifiable natural person processed by Diver on the Customer's behalf under this DPA.
- **Processing —** any operation performed on Personal Data, including collection, storage, organisation, analysis, transmission and deletion.
- **Sub-processor —** any third party engaged by Diver to process Personal Data on the Customer's behalf.
- **Data Subject —** the identified or identifiable natural person to whom Personal Data relates.
- **Supervisory Authority —** an independent public authority established by an EU Member State pursuant to Article 51 GDPR (and equivalent UK authority).
- **SCCs —** the Standard Contractual Clauses adopted by the European Commission under Implementing Decision (EU) 2021/914.
- **GDPR —** Regulation (EU) 2016/679 of the European Parliament and of the Council, and where applicable, the UK GDPR and the Data Protection Act 2018.

3. Scope & Roles

This DPA applies to the Processing of Personal Data by Diver on the Customer's behalf in connection with the Service. With respect to such Processing, the Customer is the Controller (or processor acting on behalf of its own controller) and Diver is the Processor. Each Party will comply with its respective obligations under applicable data protection law.

4. Subject Matter, Duration, Nature & Purpose

Subject matter: the provision of the Diver conversion-intelligence and reporting service.

Duration: the term of the Customer's subscription plus any post-termination retention period described in the Privacy Policy and in section 15 below.

Nature: automated and, where required, manual Processing operations including collection, storage, organisation, structuring, analysis, transmission, restriction and deletion.

Purpose: to (a) deliver and operate the Service, (b) provide customer support, (c) ensure security and detect abuse, and (d) comply with Diver's legal obligations as Processor.

5. Categories of Data Subjects

- End-users and visitors of the Customer's website (in aggregated form, via signals from connected analytics, advertising and search platforms).
- The Customer's authorised users and account holders (administrators, team members,

collaborators).
- Other individuals whose Personal Data the Customer chooses to submit to the Service.

6. Categories of Personal Data

- Account and profile data of authorised users: name, email address, IP address, country, profile picture and authentication identifiers.
- Usage and event data generated by interacting with the Service (logs, audit trail, in-product activity).
- Conversion, traffic, advertising and search-performance data drawn from the Customer's connected platforms (e.g. GA4, Google Search Console, Google Ads).
- Support correspondence (email content and metadata) when the Customer contacts Diver.

Diver does not request or knowingly process special categories of Personal Data (Article 9 GDPR) and instructs Customer not to submit such data through the Service.

7. Customer Instructions

Diver will Process Personal Data only on documented instructions from the Customer, including the Terms of Service, this DPA, and any settings configured in the application, unless required to do so by EU or Member State law. Diver will inform the Customer if it becomes aware that an instruction infringes applicable data protection law (unless prohibited by law from doing so).

8. Confidentiality

Diver ensures that personnel authorised to Process Personal Data are bound by appropriate confidentiality obligations (whether contractual or statutory), receive data protection training, and access Personal Data only on a need-to-know basis to perform their duties.

9. Security Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, Diver implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- Encryption of data in transit (TLS 1.2+) and at rest where technically feasible.
- Role-based access control with least-privilege defaults.
- Multi-factor authentication (MFA) required on all Diver administrative accounts.
- OAuth-scoped API access; Diver staff do not have direct access to Customer's raw analytics data.
- Audit logging of significant administrative and security-relevant actions.
- Regular dependency, vulnerability and patch monitoring.
- Encrypted backups with restricted access and tested restore procedures.
- Segregation of production, staging and development environments.
- Incident response and breach-handling procedures aligned with Article 33 GDPR.

The full checklist of measures is set out in Annex II.

10. Sub-processors

The Customer provides general written authorisation for Diver to engage Sub-processors to Process Personal Data, subject to the following safeguards:

- Each Sub-processor is bound by a written contract imposing data protection obligations no less protective than those in this DPA.
- Diver remains fully liable to the Customer for the performance of each Sub-processor's obligations.

Diver will provide at least thirty (30) days' notice of any intended addition or replacement of a Sub-processor (by email or in-app notification), giving the Customer the opportunity to object on reasonable data protection grounds.

- If the Customer reasonably objects, the Parties will work in good faith to find a resolution; failing which, the Customer may terminate the affected Service for convenience without penalty.

The current list of approved Sub-processors is set out in Annex III.

11. International Transfers

Where Personal Data is transferred from the EEA, Switzerland or the United Kingdom to a country that has not been recognised as providing an adequate level of protection, Diver relies on the European Commission's Standard Contractual Clauses (Module Two: controller-to-processor) and, for UK transfers, the UK International Data Transfer Addendum to those SCCs. The Parties agree that the SCCs are deemed entered into by reference and form part of this DPA. A signed copy is available on request to privacy@greenhatwebs.com.

12. Data Subject Rights

Taking into account the nature of the Processing, Diver assists the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to Data Subject requests (including access, rectification, erasure, restriction, portability and objection). The Service provides self-service export and deletion controls; for assistance beyond those tools, Diver will respond to written Customer requests within five (5) business days.

13. Data Breach Notification

Diver will notify the Customer without undue delay and in any event within 72 hours of becoming aware of a Personal Data Breach affecting the Customer's Personal Data. The notification will include, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its possible adverse effects, so that the Customer can comply with its obligations under Articles 33–34 GDPR.

14. Audits

Diver will make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for, and contribute to, audits, including inspections, conducted by the Customer or another auditor mandated by the Customer. To minimise disruption, Diver may satisfy this obligation by providing recent third-party audit reports, security certifications, or completed security questionnaires. Audits are at the Customer's expense, on at least thirty (30) days' written notice, no more than once per twelve (12) month period (except following a Personal Data Breach), and subject to reasonable confidentiality obligations.

15. Return or Deletion

Upon termination or expiry of the Service, Diver will, at the Customer's choice, delete or return all Personal Data Processed on the Customer's behalf within ninety (90) days, and delete existing copies, except to the extent that EU or Member State law requires storage of the Personal Data. The lifecycle described in the Privacy Policy (active !’ suspended !’ blocked !’ deleted) governs subscription-driven deletion within this window.

16. Liability & Precedence

In the event of any conflict or inconsistency between this DPA and the Terms of Service or any other agreement between the Parties, this DPA prevails with respect to the Processing of Personal Data.

Where the SCCs apply, the SCCs prevail over this DPA in the event of conflict. Each Party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Terms of Service.

17. Acceptance

By executing the Terms of Service, or by continuing to use the Service after the Effective Date, the Customer accepts this DPA. Where a signed counterpart is required for the Customer's records, the Customer may sign and return a copy to privacy@greenhatwebs.com and Diver will counter-sign and return it.

Annex I — Description of Processing

The following table describes the Processing carried out by Diver on the Customer's behalf, in accordance with Article 28(3) GDPR and Clause 8 of the SCCs.

Item	Details
Categories of Data Subjects	Customer's authorised users (account holders, administrators, team members); end-users of the Customer's website (in aggregated analytics form); other individuals whose Personal Data the Customer chooses to submit to the Service.
Categories of Personal Data	Account and profile data (name, email, IP, country, profile picture); authentication identifiers; usage and audit-log data; conversion, traffic, advertising and search-performance data drawn from the Customer's connected platforms; support correspondence.
Special categories of data	None. The Service is not designed to Process special categories of Personal Data.
Nature of Processing	Collection, storage, organisation, structuring, analysis, transmission, restriction and deletion, performed primarily by automated means.
Purposes of Processing	Provision and operation of the Service; customer support; security, abuse and fraud prevention; compliance with legal obligations.
Duration of Processing	For the term of the Customer's subscription, plus the post-termination retention window described in section 15 (up to 90 days for return or deletion).
Retention	Personal Data is retained for the duration of the subscription. Following termination, Personal Data is deleted or returned within 90 days, except where law requires longer retention. Audit logs may be retained for up to 12 months for security purposes.
Frequency of transfers	Continuous, for as long as the Customer uses the Service.

Annex II — Technical & Organisational Measures

The following measures are implemented by Diver and correspond to the security commitments in section 9 of this DPA.

Measure	Description
Encryption in transit	All connections use TLS 1.2 or higher. HSTS is enforced on production endpoints.
Encryption at rest	Production databases and backups are encrypted at rest where technically feasible.
Access control	Role-based access with least-privilege defaults; access reviewed periodically and revoked on personnel changes.
Multi-factor authentication	MFA is required on all Diver administrative accounts and on all production-system access.
OAuth-scoped data access	Customer analytics data is accessed via OAuth scopes granted by the Customer; Diver staff do not have direct access to raw analytics data.
Audit logging	Significant administrative and security-relevant actions are logged and retained for review.
Vulnerability management	Continuous dependency monitoring; security patches applied on a risk-prioritised basis.
Backups	Automated, encrypted backups with restricted access and tested restore procedures.
Environment separation	Production, staging and development environments are logically segregated; production data is not used in non-production environments.
Incident response	Documented incident response and breach-notification procedures aligned with Article 33 GDPR (see section 13).
Personnel	Confidentiality obligations and data protection training for personnel with access to Personal Data.

Annex III — Approved Sub-processors

The following Sub-processors are currently engaged by Diver to Process Personal Data on the Customer's behalf.

Name	Service	Location
Replit, Inc.	Cloud application hosting and database infrastructure.	United States
Stripe, Inc.	Payment processing and billing.	United States
Google LLC	OAuth identity and API access to GA4, Google Search Console and Google Ads (data remains under the Customer's Google account).	United States / EU
SMTP2GO	Transactional email delivery (account, security and product notifications).	United States / EU