Reditus Data Processing Agreement

Version 1.0. Effective 4 August 2026.

The undersigned:

the Customer, being _____ with its registered office at _____, registered with the Chamber of Commerce under number _____ and legally represented by _____ ("Customer");

and

Reditus B.V., with its registered office at Kapelweg 12, 3951 AC Maarn, Netherlands, registered with the Dutch Chamber of Commerce (KvK) under number 77814487, VAT number NL861156420B01, legally represented by Joran Hofman (Founder) ("Reditus");

have agreed as follows.

Preamble

This Data Processing Agreement ("DPA") sets out the terms on which Reditus processes personal data on behalf of the Customer in providing the Reditus affiliate and partner marketing platform, and identifies the processing Reditus carries out as controller in its own right. It contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (EU) 2016/679. It is incorporated by reference into the Reditus Terms of Service and applies automatically to every Customer; the signature block explains how to obtain a countersigned copy.

1. Definitions and interpretation

1.1 "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" have the meanings given in Data Protection Law.

1.2 "Data Protection Law" means, as applicable: the GDPR; the Dutch Uitvoeringswet AVG; the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025; the Swiss Federal Act on Data Protection (the "FADP"), overseen by the Swiss Federal Data Protection and Information Commissioner (the "FDPIC"); and the US State Privacy Laws, including the California Consumer Privacy Act as amended (the "CCPA").

1.3 "Customer Personal Data" means personal data Reditus processes on behalf of the Customer in providing the Services, including data the Customer or its users upload, data collected through the Reditus tracking script on the Customer's own websites, and data received from systems the Customer connects. Annex A1 describes it.

1.4 "End Client" means the controller on whose behalf the Customer, itself acting as a processor, processes personal data, and in respect of which Reditus acts as a sub-processor.

1.5 "Privacy Contact" means the Reditus address for data protection notices, Sub-processor objections and assistance requests: `privacy@getreditus.com`.

1.6 "Restricted Transfer" means a transfer of personal data to a country outside the EEA, the United Kingdom or Switzerland, as applicable, that is only permitted under Data Protection Law if a transfer safeguard is in place.

1.7 "Service Data" means personal data Reditus processes as a controller in its own right in connection with the Services, as described at Annex A2.

1.8 "Services" means the Reditus affiliate and partner marketing platform and any related service provided under the Terms of Service.

1.9 "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, as incorporated and completed at clause 8.

1.10 "Sub-processor" means any processor engaged by Reditus, or by another Sub-processor, to process Customer Personal Data; the approved list is at Annex C, maintained at `https://www.getreditus.com/sub-processors`.

1.11 "Terms of Service" means the Reditus Terms of Service at `https://www.getreditus.com/terms-of-service`, together with any order form or other written agreement for the Services.

1.12 This DPA is incorporated into the Terms of Service and its Annexes form part of it. "Including" means "including without limitation", and a reference to a statute is to it as amended or replaced.

2. Roles and scope

2.1 For Customer Personal Data, the Customer is the controller and Reditus the processor. Where the Customer is itself a processor acting for an End Client, Reditus is a Sub-processor, this DPA applies as if references to the controller were references to the End Client, and the Customer confirms it holds the authorisations needed to engage and instruct Reditus on the End Client's behalf.

2.2 Reditus is an independent controller for Service Data: account administration, billing, security and fraud prevention, product analytics and error diagnostics concerning use of the Services, and compliance with its own legal obligations. Reditus is also an independent controller for the profiles in its own affiliate network, marketplace and recruitment database, until an affiliate joins the Customer's programme, from which point the data inside that programme is Customer Personal Data and Reditus is the Customer's processor for it. Annex A2 describes both activities, which are governed by the Reditus privacy notice rather than by the Customer's instructions. Reditus records sessions solely for error monitoring and bug diagnosis, and is rolling out masking and exclusion rules so that telemetry, error payloads and session recordings contain no personal data. To the extent any Customer Personal Data is captured, it is Customer Personal Data, not Service Data. Nothing in this clause permits Reditus to use Customer Personal Data for its own purposes; clause 10 governs anonymised aggregates.

2.3 The Customer is the controller of its own websites and applications. The Customer, not Reditus, decides whether the Reditus tracking script and its cookies require consent where the Customer operates, obtains that consent where required, and describes the cookies in its own cookie notice; Annex A1 publishes each cookie's name, purpose and lifetime to enable this.

2.4 Reditus processes Customer Personal Data only on the Customer's documented instructions, including for transfers to a third country or an international organisation. The documented instructions are this DPA, the Terms of Service, the Customer's use and configuration of the Services (settings, integrations, the data it sends), and any further lawful written instruction that is technically feasible and consistent with the Services. The Customer controls what personal data it sends: in UID mode the Customer sends only an opaque internal identifier through the tracking script and the Reditus API instead of an email address or name, so that no directly identifying data about referred persons reaches Reditus at all (Annex A1, "Zero-PII UID mode"). The Customer can also integrate entirely server side, reporting both referrals and payments through the Reditus API with unique identifiers only and without installing the tracking script, in which case Reditus processes no personal data about the Customer's clients whatsoever.

2.5 If Union or Member State law requires Reditus to process Customer Personal Data other than on the Customer's instructions, Reditus will inform the Customer of that requirement before processing, unless the law prohibits it on important grounds of public interest.

2.6 Reditus will immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Law, and may pause the processing concerned until the Customer confirms, withdraws or amends the instruction.

2.7 The Services are not designed for special categories of personal data (Article 9 GDPR), criminal offence data (Article 10 GDPR) or the personal data of anyone under 18, and the Customer must not send them. If such data nonetheless arrives, Reditus protects it under Annex B, tells the Customer as soon as it becomes aware, and deletes or returns it on instruction.

3. Personnel and confidentiality

3.1 Reditus keeps Customer Personal Data confidential and discloses it only to its authorised personnel, to Sub-processors under clause 9, and where required by law under clause 7. This obligation survives the end of the Terms of Service without limit of time.

3.2 Everyone who may access Customer Personal Data on Reditus's behalf, including employees, directors, contractors, freelancers, temporary and agency staff, and external providers working on Reditus's own systems, signs a non-disclosure agreement, or is bound by an appropriate statutory confidentiality obligation, before access is granted; the obligation survives the engagement, and they are informed of their duties under Data Protection Law and this DPA.

3.3 Reditus limits access to Customer Personal Data to personnel who need it for a defined task, removes access promptly on role change or departure, and will provide data protection and security awareness training to personnel with access.

4. Security

4.1 Reditus implements and maintains appropriate technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure and unauthorised access, as Article 32 GDPR requires, including the measures in **Annex B**.

4.2 Reditus may update the measures in Annex B as technology and threats change, and may replace an individual measure, provided the replacement is equivalent or stronger and the overall level of security does not fall below the standard described in that Annex.

4.3 Reditus applies the principles of data protection by design and by default to its product and features. Concrete outputs of that approach in the current Services: **full server-side integration** (the Customer can report referrals and payments through the Reditus API using only opaque unique identifiers, without installing the tracking script at all, in which case Reditus receives no personal data about the Customer's own clients and the only personal data processed is the account data of the Customer's own users); **UID mode** with the tracking script, where the Customer elects it: no directly identifying data about referred persons then reaches Reditus (without UID mode, the referred person's email address is typically sent for attribution); **client IP addresses truncated at the point of collection** in referral event records; no device fingerprinting in the tracking script; configurable cookie lifetime; and partial masking of email addresses shown to affiliates.

4.4 Security at the Customer's end is the Customer's responsibility. In particular, the Customer keeps its API keys, tokens, passwords and other credentials for the Services confidential and rotates them if compromise is suspected, secures the devices, systems and websites from which the Services are accessed or on which the tracking script runs, and applies the principle of least privilege to its own users' access to the Services.

5. Assistance

5.1 Affiliate records, referred-lead records and the associated tracking and commission data are designed to be findable and exportable inside the platform. Deletion of an individual record is handled by Reditus on request, free of charge, within the timescales in clause 5.2.

5.2 Taking into account the nature of the processing, Reditus will assist the Customer, by appropriate technical and organisational measures, in responding to data subject requests: access, rectification, erasure, restriction, portability, objection, withdrawal of consent, and Article 22 GDPR requests concerning automated decision-making. Reditus acknowledges an assistance request within 2 business days, responds substantively within 5, and where the Customer works to a one month deadline under Article 12(3) GDPR, in time to meet it.

5.3 If a data subject contacts Reditus directly about Customer Personal Data, Reditus will not respond substantively; it confirms receipt, refers the person to the Customer, and forwards the request to the Customer within 5 business days.

5.4 Reditus will give reasonable assistance with data protection impact assessments (Article 35 GDPR), prior consultation (Article 36 GDPR), the Customer's obligations under Articles 32 to 34 GDPR, and supervisory authority enquiries concerning the processing in Annex A1.

5.5 Ordinary assistance under this clause is free. Reditus may charge a reasonable fee where a request is manifestly unfounded, excessive or repetitive, or requires more than eight person-hours of engineering time in any twelve month period; it gives a written estimate first, starts no chargeable work without written approval, and never uses cost to delay assistance needed for a statutory deadline.

6. Personal Data Breach

6.1 Reditus will notify the Customer of a Personal Data Breach affecting Customer Personal Data without undue delay, and in any event within **48 hours** of becoming aware of it, so that the Customer can meet its own 72 hour deadline under Article 33(1) GDPR. Awareness begins when any member of Reditus personnel has a reasonable degree of certainty that such an incident has occurred; internal triage does not postpone it.

6.2 So far as available, the notification describes the nature of the breach, the categories and approximate numbers of data subjects and records concerned, the likely consequences, the measures taken or proposed, and the Reditus contact point; anything not yet available follows in phases without further undue delay.

6.3 Reditus will provide a written root cause analysis within **30 days of containment** and will cooperate with the Customer's investigation, mitigation and notifications.

6.4 Reditus will not notify a supervisory authority or data subjects on the Customer's behalf unless the Customer instructs it or the law requires it, in which case Reditus tells the Customer first where lawful. A notification under this clause is not an admission of fault. Unsuccessful attempts that do not compromise Customer Personal Data, such as port scans, failed logins and blocked denial of service attempts, are not individually notified.

7. Government requests

If a public authority, court or law enforcement body requests Customer Personal Data, Reditus will first attempt to redirect the requester to the Customer as controller, and will notify the Customer promptly unless legally prohibited, in which case it will use reasonable efforts to obtain a waiver so it can share what it lawfully can, as soon as it lawfully can. Reditus reviews each request, challenges one that appears unlawful, overbroad or not issued under a valid legal procedure, and suspends disclosure while a challenge is pending where lawful. If compelled, Reditus discloses only the minimum necessary, keeps a record of every binding request, and shares information about them with the Customer to the extent lawfully permitted. Reditus provides no government with direct, unrestricted or bulk access to Customer Personal Data and hands over no encryption keys for that purpose.

8. Cross-border transfers

8.1 The production data store for Customer Personal Data is in the European Union: the application runs on Hetzner Online GmbH infrastructure in Nuremberg, Germany, and the primary database, authentication and file storage are provided by Supabase Pte. Ltd in an EU region (Frankfurt, Germany). Supabase contracts through a Singapore entity, so that leg relies on the Standard Contractual Clauses rather than on data location alone. A few Sub-processors process limited categories outside the EEA or under a non-EEA contracting entity; Annex C names each and its transfer mechanism.

8.2 The Standard Contractual Clauses are incorporated by reference and apply to every Restricted Transfer of Customer Personal Data, completed as follows. Module Two applies where the Customer is a controller; Module Three where the Customer is a processor acting for an End Client. The optional

docking clause at Clause 7 is enabled. Under Clause 9(a), Option 2 (general written authorisation) applies, with the 30 day notice period and objection mechanics in clause 9 of this DPA. The optional language in Clause 11 is not used. Under Clause 13 and Annex I.C, the competent supervisory authority is that of the EEA Member State in which the data exporter is established or, for an exporter not established in the EEA but within Article 3(2) GDPR, the authority determined under Clause 13(a); Clause 13 does not operate under Module Four. Under Clause 17 the Clauses are governed by Netherlands law; under Clause 18 disputes go to the courts of the Netherlands. Annex I of the Clauses is completed by the party details in this DPA and Annex A1; Annex II by Annex B; Annex III by Annex C. Where Reditus returns or discloses Customer Personal Data to a Customer established outside the EEA and outside an adequate country, Module Four applies to that leg with the same completions so far as they are capable of applying to that Module. Acceptance of the Terms of Service constitutes signature of the Standard Contractual Clauses, including their Annexes, by both parties.

8.3 For transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the Information Commissioner, is incorporated by reference; its tables are deemed completed with the information in this DPA, and either party may end it as set out in Section 19 of its Mandatory Clauses.

8.4 For transfers subject to the FADP, the Clauses apply as amended for Switzerland: the competent supervisory authority is the FDPIC, references to the GDPR are read as the FADP to the extent it governs the transfer, data subjects in Switzerland may bring proceedings there, and, if and to the extent the FADP again protects data relating to legal entities, the Clauses apply to that data on the same terms.

8.5 If an adequacy decision that a transfer relies on is invalidated, suspended or lapses, the Standard Contractual Clauses apply to that transfer automatically from that date, without further action by either party. Where a Sub-processor also holds an EU-US Data Privacy Framework certification, Annex C records it as a supplementary fact only; the Clauses remain the mechanism relied on.

9. Sub-processors

9.1 The Customer gives Reditus a general written authorisation to engage the Sub-processors listed at **Annex C** and any Sub-processor added under this clause. This clause governs only Sub-processors, that is vendors that process Customer Personal Data; tools Reditus uses for its own business that never touch Customer Personal Data are not Sub-processors and can change without notice under this clause.

9.2 At least **30 days** before a new Sub-processor begins processing Customer Personal Data, Reditus will publish a dated update in the Reditus trust centre updates feed, update the published list, **and** email the Customer's designated privacy or administrative contact. The objection window runs from whichever notice arrives last. The Customer keeps its designated contact current in the Services.

9.3 The Customer may object within **14 days**, on reasonable grounds relating to data protection, by writing to the Privacy Contact. Reditus will work in good faith to resolve the objection, and will not permit the objected-to Sub-processor to process that Customer's data while it is unresolved. If the objection cannot be resolved within 30 days, the Customer may terminate the affected part of the Services (or, where it cannot reasonably be separated, the whole of the Services) on written notice,

without penalty, with a pro-rated refund of prepaid fees covering the period after termination. Reditus is not obliged to abandon a planned change for other Customers; termination with the refund above is the Customer's remedy.

9.4 Where a change of Sub-processor is needed urgently to preserve the availability, security or integrity of the Services, or because an existing Sub-processor stops providing its service, Reditus may appoint a replacement immediately and give notice as soon as practicable, stating why advance notice was not practicable; the 14 day objection window then runs from that notice and clause 9.3 applies in full.

9.5 Before a Sub-processor begins processing, Reditus will enter into a written contract imposing the same data protection obligations as set out in this DPA, and in any event obligations no less protective, in particular sufficient guarantees of appropriate technical and organisational measures, including the applicable transfer safeguard where the Sub-processor is outside the EEA. Reditus maintains such contracts with the Sub-processors listed in Annex C; execution of the last of these agreements is in progress at the date of this version and is being completed now.

9.6 Where a Sub-processor fails to fulfil its data protection obligations, Reditus remains fully liable to the Customer for those obligations, as Article 28(4) GDPR requires.

10. AI and anonymised aggregates

Reditus does not use Customer Personal Data to train, fine-tune or otherwise improve any general-purpose AI model, foundation model or other machine learning model, whether its own or a third party's, and does not permit any Sub-processor or AI service provider to do so. Any AI service provider that processes Customer Personal Data is a Sub-processor, will be named in Annex C under the notice procedure in clause 9 before it begins or continues processing, and will be bound to terms that prohibit training on Customer Personal Data and require zero retention or a short, stated retention period for abuse monitoring only. No AI vendor processes Customer Personal Data today: Reditus's AI recruitment and discovery features operate on Reditus's own side of the role split in clause 2.5, processing Reditus's affiliate network and recruitment data as controller, using Google's Gemini API for classification and matching (under the Google Cloud Data Processing Addendum; prompts and outputs are not used to train Google's models), DataForSEO OU for public web and search data about candidate sites and companies (no personal data is sent to or returned by it in that pipeline), and Hunter Web Services, Inc. to find and verify work email addresses (the personal data in that step being the candidate's name, email address and LinkedIn profile). Those vendors are disclosed in the Reditus privacy notice and on the corporate list of the sub-processor page, and none of them receives Customer Personal Data. Where the Services produce a score, match, ranking or suggestion about a person, that output is provided for the Customer to act on: Reditus does not make decisions producing legal or similarly significant effects on data subjects on the Customer's behalf.

Reditus may create irreversibly anonymised, aggregated data from Customer Personal Data to operate, secure, analyse and improve the Services and to produce benchmarks, only where no individual can be singled out, linked or inferred. Reditus will not attempt re-identification, will not use aggregation as a route around the training prohibition above, will not publish any statistic derived from fewer than 20 Customers or 20 programmes, and will not publish or disclose aggregated data in a

form that identifies the Customer, its affiliates, its leads or its referred customers without the Customer's prior written consent.

11. Data subject requests and third-party rights

11.1 Data subject requests that reach Reditus directly are handled and forwarded under clause 5.3; Reditus cooperates with supervisory authority enquiries concerning Annex A1 processing under clause 5.4.

11.2 Except for data subjects' rights under the Standard Contractual Clauses and Data Protection Law, no third party may enforce this DPA.

12. Term and termination

This DPA takes effect on the effective date above, or when the Customer first accepts the Terms of Service if later, and remains in force for as long as the Terms of Service do, and thereafter for as long as Reditus processes Customer Personal Data. Any provision that should by its nature survive to protect Customer Personal Data survives termination.

13. Data return and destruction

13.1 On the Customer's written request, and in any event on termination or expiry of the Terms of Service, Reditus will, at the Customer's choice, either return Customer Personal Data or delete it, and will then delete existing copies unless Union or Member State law requires retention.

13.2 The Customer can export its data using the export features of the platform during the term and for **60 days** after termination or expiry, during which Reditus keeps the account read-only at no charge. On request, Reditus provides Customer Personal Data in a structured, commonly used, machine-readable format such as CSV or JSON within 30 days; the same export path serves Article 20 GDPR portability. Reditus completes the chosen return or deletion within 30 days of the Customer's choice, or within 30 days of the end of the export window if no choice is made, and in any event deletes Customer Personal Data from live systems no later than **120 days** after termination or expiry.

13.3 Customer Personal Data may remain in backups after deletion from live systems, because backups are overwritten on a rolling **7 day** cycle rather than edited. Data in backup is isolated from production, used for nothing, and restored only for disaster recovery, in which case Reditus re-applies the deletion. Reditus confirms deletion in writing on request.

13.4 Where law requires retention, for example for tax or accounting, Reditus retains only what the law requires, for as long as it requires, tells the Customer what and why, and processes it for no other purpose. Retention periods per category are in the schedule at Annex A1.

14. Records and audit

14.1 Reditus maintains the Article 30(2) GDPR record of categories of processing carried out for the Customer and makes the relevant part available to the Customer or a supervisory authority on request.

14.2 On written request, no more than once in any twelve month period unless Data Protection Law requires otherwise or following a material change to Annex B or Annex C, Reditus will make available the information needed to demonstrate compliance with Article 28 GDPR and this DPA: Annex B, the current Sub-processor list, the security overview at `https://www.getreditus.com/security`, and written responses to a reasonable security questionnaire within 15 business days.

14.3 Reditus will allow for and contribute to audits, including inspections, by the Customer or an auditor it mandates. Reditus is fully remote and has no facility of its own in which Customer Personal Data is processed, so an inspection is conducted remotely, by video conference and document review; for assurance about a Sub-processor's data centre, Reditus passes the request on and shares what its contract allows. An inspection requires 30 days' written notice, runs at most once in any twelve month period, and is subject to confidentiality; that limit, and the limit in clause 14.2, do not apply where a supervisory authority requires it or after a confirmed Personal Data Breach affecting the Customer's data. The Customer bears its own costs and the reasonable costs of Reditus's time beyond what Reditus already publishes; the auditor may not be a competitor whose principal business is affiliate, referral or partner-marketing software.

15. Warranties

15.1 Reditus warrants that it and anyone acting on its behalf will process Customer Personal Data in compliance with Data Protection Law and this DPA.

15.2 The Customer warrants that it has and will maintain a lawful basis for the processing it instructs, that the required notices have been given and any required consents obtained, and that its instructions comply with Data Protection Law.

16. Liability

Each party's total aggregate liability arising out of or in connection with this DPA is limited to the greater of the limit of liability in the Terms of Service and the fees paid or payable by the Customer in the twelve months before the first event giving rise to the liability; liability under this DPA is capped, not excluded, and no exclusion of liability in the Terms of Service applies to it. Nothing in this DPA or the Terms of Service limits either party's liability for a breach of Data Protection Law to the extent the law does not permit it to be limited, including liability to data subjects under Article 82 GDPR. The applicable cap limits, but does not disclaim, Reditus's responsibility for its Sub-processors under Article 28(4) GDPR.

17. US state privacy laws

Where Reditus processes personal information subject to a US State Privacy Law on the Customer's behalf, Reditus is the service provider or processor, the Customer the business or controller, and the disclosure of personal information to Reditus is neither a sale nor a share. Reditus will not sell personal information or share it for cross-context behavioural advertising; will not retain, use or disclose it for any purpose other than providing the Services, or outside the direct business relationship; and will not combine it with personal information from another source, except in each case where the applicable law expressly permits it. Reditus certifies that it understands these restrictions and will comply with

them, and will notify the Customer if it can no longer do so, upon which the Customer may take reasonable steps to stop and remediate unauthorised use. Where Reditus creates deidentified data it will not attempt to reidentify it and will bind recipients to the same; the advertising and analytics on Reditus's own websites is Reditus's own controller processing, disclosed in the Reditus privacy notice, not processing on the Customer's behalf.

18. Order of precedence, amendments, applicable law and venue

18.1 For the processing of personal data, this DPA prevails over the Terms of Service to the extent of any conflict; executed Standard Contractual Clauses prevail over this DPA for the transfers they cover.

18.2 Reditus may amend this DPA; each version carries a version number and an effective date. Reditus will give at least 30 days' notice, by email to the Customer's designated contact and by an update in the Reditus trust centre, of any amendment that materially reduces the Customer's rights; the Customer may object on reasonable data protection grounds and, if the objection is not resolved within 30 days, terminate on the terms in clause 9.3. Changes required by Data Protection Law take effect when the law requires. Where the Customer has signed an order form, the version in effect on its date applies for its term, except for changes required by law. Nothing in this clause varies the Standard Contractual Clauses.

18.3 This DPA and its execution are governed by Dutch law. The Rechtbank Midden-Nederland has exclusive jurisdiction over any dispute arising out of or in connection with this DPA, without affecting the forum elected in the Standard Contractual Clauses or a data subject's right to bring proceedings where Data Protection Law allows.

Signature block

No Customer signature is needed. This DPA is incorporated by reference into the Terms of Service and applies automatically; acceptance in electronic form satisfies Article 28(9) GDPR. Reditus has signed it in advance; a Customer that needs a countersigned copy can request one from the Privacy Contact with its legal entity name, registered address and company number.

Signed for **Reditus B.V.**: Joran Hofman, Founder, at Maarn, Netherlands, on 4 August 2026.

Signed for the **Customer** (only where a countersigned copy is requested):

Name: _____ Title: _____

Date: _____ Signature: _____

Annex A1: Processing activities where Reditus is Processor or Sub-processor

Type	Description
Business purposes	Providing the Services as described in the Terms of Service.

Type	Description
Subject matter	Operating the Customer's affiliate, referral or partner programme: enrolling and managing affiliates and advocates, tracking clicks and referrals, attributing signups and purchases to the referring affiliate, calculating commissions, executing payouts.
Nature	Collection, recording, storage, retrieval, use, disclosure by transmission to the Sub-processors in Annex C and to systems the Customer connects, alignment, restriction, erasure, destruction.
Purpose	Account administration; affiliate enrolment and verification; tracking and attribution; commission calculation and payout execution; fraud, self-referral and duplicate detection; programme reporting; transactional email; support; marketplace listing where enabled; platform security and integrity.
Duration	The term of the Terms of Service, then only for the periods in the retention schedule below.
Frequency	Continuous; tracking and attribution events are processed in real time.
Sensitive data	None. The Services are not designed for Article 9 or Article 10 data or the data of anyone under 18, and clause 2.7 instructs the Customer not to transmit them.
Obligations and rights of the Customer	As set out in this DPA, in particular clauses 2, 5, 13 and 14, and in the Terms of Service: the Customer determines the purposes and means, owns the lawful basis, the data subject notices and the cookie-consent decision for its own websites, and decides what data its website transmits to Reditus.

Data subject groups.

Group	Data categories	Source
Customer personnel and account users	Name; business email address; authentication credentials (stored only as hashes); company name and domain; role and permissions; IP address; session timestamps; in-product activity; support content; billing contact details and subscription status. Reditus does not receive or store payment card numbers: card details go directly to Stripe Payments Europe, Limited.	The Customer, at signup and in the product.
The Customer's affiliates and advocates	Name; email address; company name, website and domain; affiliate and advocate identifiers; authentication credentials (stored as hashes); IP address; tracking UUID; commission balances and payout history; **payout identifiers, being the PayPal email address used for payouts and, where the affiliate requests SEPA payment, the affiliate's IBAN**; marketing channels and profile information where supplied; support messages; read-only data from connected accounts (YouTube, Google Analytics 4), revocable by the affiliate.	The affiliate directly; the Customer, where it invites or imports affiliates; the affiliate's connected accounts.

Group	Data categories	Source
Leads and customers referred through a tracked link	The tracking UUID (a random version 4 UUID generated in the visitor's browser, held in the `_gr_id` first-party cookie); IP address; click and referral events including the referrer and the full page address with its query string; the Customer's own opaque `uid` where sent; email address and name where the Customer chooses to send them; subscription and transaction events from the Customer's connected Stripe account; calculated commission amounts.	The Customer's website and product via the tracking script; the Customer's Stripe account; the Customer's systems via the Reditus API and webhooks.

Passthrough. The tracking script transmits whatever parameters the Customer configures it to send: there is no fixed allowlist of meta parameters, and the full page address including its query string is transmitted, so the Customer decides what personal data reaches Reditus. Where the Customer runs the Reditus script and a HubSpot form or meetings widget on the same page, the integration transmits the end user's email address by default; a Customer that does not want that disables the integration or uses UID mode.

Zero-PII UID mode. In UID tracking the Customer sends an opaque internal identifier instead of an email address or name, and Reditus attributes referrals and calculates commissions without receiving any directly identifying value about referred persons. Taken to its full extent, the Customer can integrate entirely server side: referrals and payments are reported through the Reditus API with unique identifiers only, no tracking script is installed on the Customer's website, and Reditus receives no personal data about the Customer's clients at all. In that configuration the only personal data Reditus processes is the account data of the Customer's own users (group (i)).

Cookies set by the tracking script: `_gr_id` (referral attribution, random UUID plus captured campaign values, 60 days by default, configurable 1 to 120 days); `_gr_cookietest` (cookie-support check, no personal data, transient); `_gr_referral_widget` (referral widget where enabled, advocate contact details and a widget token, 30 days).

Retention schedule. Where a period is marked open, Reditus retains that category no longer than necessary for the purposes above, and in any event deletes or irreversibly anonymises it within 12 months after the end of the Terms of Service (backups: 12 months from the backup date, subject to row 9), subject to clause 13.4.

#	Category	Retention
1	Customer account and user records	For the life of the Customer account, because the records power the Customer's and affiliates' dashboards and reporting. On termination, exported and deleted under clause 13 (60 day export window, deletion within the 120 day longstop); earlier deletion on request to the Privacy Contact.
2	Affiliate and advocate records	Deleted with the programme or the account: when a programme is deleted, everything related to it, including advocate and enrolment records, is deleted with it.
3	Raw click, visit and referral events	Client IP addresses are truncated at the point of collection. Event records are retained for the life of the account and deleted with it, because they underlie the Customer's and affiliates' reporting.

#	Category	Retention
4	Conversion, subscription and commission records	Raw Stripe webhook payloads: deleted once older than **1 month**. Derived conversion and commission records: for the life of the programme and account (they underlie commission calculations and dashboards), then deleted under rows 1 and 2. Where a commission links to a payment receipt, Reditus stores only a link into the Customer's own Stripe account, shown to the Customer alone; the receipt itself is not stored by Reditus.
5	Payout identifiers (PayPal email address, IBAN)	Deleted when the affiliate is deleted; affiliates can also remove their own payout details at any time in their account.
6	Payout transaction records	Until the account holder deletes their account; records that form part of Reditus's own statutory accounting are kept for 7 years under Dutch law.
7	Support conversations	For the duration of the relationship, in an EU-established support tool (CORDNET OU, Estonia); deleted with the account or on request.
8	Product analytics, error diagnostics and session recordings	Session recordings: deleted after the recording retention window configured in the analytics tool (30 days standard, at most 90). Analytics and error events: retained while the account is active, deleted with it.
9	Backups	**7 days**: daily snapshots with rollback to any day in the preceding 7 days; deleted data ages out with that window. No longer-term or off-platform archive exists (confirmed 4 August 2026).
10	Cookies set by the tracking script	`_gr_id` 60 days by default (configurable 1 to 120 days); `_gr_cookietest` transient; `_gr_referral_widget` 30 days

Annex A2: Processing activities where Reditus is a Controller

Type	Description
Service Data	Account administration, billing and invoicing, security and fraud prevention, product analytics and error diagnostics concerning the use of the Services, and compliance with Reditus's own legal obligations. Reditus decides the purposes and means and is accountable in its own right.
Network, marketplace and recruitment-database profiles	Profiles in the Reditus affiliate network, marketplace and recruitment database, until an affiliate joins the Customer's programme. Two populations: **registered affiliates**, who created a Reditus account and accepted the Reditus affiliate terms, and **non-registered candidates**, compiled from publicly available sources, whose Article 14 notice is section 6 of the Reditus privacy notice.
Data subject types	Customer account users (Service Data); affiliates and candidate affiliates in the Reditus network (profiles).
Duration	As set out in the Reditus privacy notice.
Governing document	The Reditus privacy notice at `https://www.getreditus.com/privacy-policy`. This processing is not on the Customer's instructions and not governed by this DPA; it is described here for transparency about marketplace profiles.

Annex B: Security measures

Technical and organisational measures protecting Customer Personal Data, stated as they exist today.

Type	Description
Physical access controls	Reditus operates no data centre and has no facility of its own; production data resides in the facilities of the infrastructure providers in Annex C. Hetzner Online GmbH holds ISO/IEC 27001:2022, certified by SOCOTEC Certification Deutschland GmbH, covering its hosting services and data centres; Supabase Pte. Ltd states that it holds SOC 2 Type 2 and ISO/IEC 27001. Those certifications belong to those providers: **Reditus holds no security certification of its own** and does not present a provider's certificate as its own.
Encryption in transit	All Reditus web properties, the application, the API and the tracking endpoint are served over HTTPS; TLS is terminated at the Cloudflare edge.
Encryption at rest	Customer Personal Data at rest is held in the managed database and object storage, which apply encryption at rest to the underlying storage media. This protects the storage media; it does not prevent access by the infrastructure providers in Annex C and does not stop an attacker holding an authorised application session.
Authentication	Authentication is token-based; session tokens are stored only as BCrypt hashes and are invalidated after two weeks. Passwords are stored only as bcrypt hashes in Reditus's own database.
Access control and least privilege	The platform enforces role-based separation between merchant users and affiliates, with permissions at user and organisation level; a Customer's users see only their own account, and an affiliate only their own referrals, commissions and payouts. Personnel access to production is limited to those who need it for their role and removed promptly on role change or departure.
Data segregation	Customer data is logically segregated per account through application-level access controls.
Pseudonymisation and minimisation	The `_gr_id` referral identifier is a randomly generated version 4 UUID created in the visitor's browser, derived from nothing about the visitor or their device. The tracking script and referral widget perform no device fingerprinting. UID mode (Annex A1) lets a Customer run a complete programme without sending any directly identifying data about referred individuals.
Output minimisation	Reditus's design intent is that affiliates receive the fact of a referral and its conversion status, with the referred person's email address partially masked rather than exposed in full. This is design intent: it has not yet been verified on every affiliate-facing surface and is not asserted as a verified control.
Integrity of commission records	Commission approvals and payout state changes are recorded as discrete, timestamped state transitions, so a commission's history can be reconstructed rather than only its current value.
Build pipeline	Changes go through version-controlled repositories and continuous integration; staging deploys automatically, production is a manual, deliberate action. Every build runs static security testing (Brakeman), dependency vulnerability scanning (Bundler Audit) and linting, plus a test suite with 95.57% line coverage.

Type	Description
Rate limiting and abuse controls	Application-level rate limiting applies to inbound requests. The platform performs fraud detection on referral events, including self-referral and duplicate detection; IP address is processed for these purposes, not to build cross-site profiles.
Edge protection	All Reditus properties sit behind Cloudflare, providing DNS, reverse proxying and network-layer DDoS mitigation.
Backups	Daily snapshots of the production database with rollback to any day in the preceding 7 days, taken by the managed database service.
Monitoring	Application errors, exceptions and performance anomalies are captured by the monitoring services in Annex C and reviewed by engineering.
Incident response	Personal Data Breaches are handled under clause 6: notification within 48 hours of awareness, written root cause analysis within 30 days of containment.

Reditus may replace any individual measure as clause 4.2 provides. Planned improvements are published at `https://www.getreditus.com/security` and move into this Annex only when implemented.

Annex C: Approved Sub-processors

Sub-processors of Customer Personal Data, as maintained at `https://www.getreditus.com/sub-processors`.

Name (legal entity)	Purpose	Location	Transfer mechanism
Hetzner Online GmbH	Hosting of the application, API and supporting infrastructure	Nuremberg, Germany	None (EEA)
Supabase Pte. Ltd	Primary database, authentication and file storage	Frankfurt, Germany (Singapore contracting entity)	SCCs, Module Three (no Singapore adequacy decision; data rests in the EU)
Cloudflare, Inc.	DNS, CDN, TLS termination and edge compute	Global edge network; TLS terminates at the point of presence nearest the visitor	SCCs, Module Three; EU-US Data Privacy Framework self-certification as a supplementary fact
Stripe Payments Europe, Limited	Payment processing and, where the Customer connects its Stripe account, reading transaction data to attribute commissions	European Economic Area	None (EEA) at the top level
PayPal (Europe) S.à r.l. et Cie, S.C.A.	Affiliate commission payouts, the default payout rail	European Economic Area	None (EEA)
Wise Europe SA	SEPA and IBAN affiliate payouts, on request	European Economic Area	None (EEA)
Twilio Inc., trading as Twilio SendGrid	Transactional email sent by the Services	United States	SCCs, Module Three

Name (legal entity)	Purpose	Location	Transfer mechanism
Functional Software, Inc., doing business as Sentry	Application error tracking and diagnostics, including session replay on the authenticated application	United States (Sentry US region)	SCCs, Module Three; EU-US Data Privacy Framework self-certification as a supplementary fact
PostHog, Inc.	Product and website analytics, including session replay on the authenticated application	Frankfurt, Germany, at rest; United States contracting entity	SCCs, Module Three (data rests in the EU; US contracting entity)
Honeybadger Industries LLC	Backend error tracking, performance monitoring and application logging	United States	SCCs, Module Three
Plane Software, Inc.	Issue tracking (hosted cloud service); tickets created from error reports can inherit personal data from the error payload	United States (hosted on Amazon Web Services)	SCCs, Module Three
CORDNET OU, trading as Featurebase	In-product support chat and product feedback	Netherlands, Germany and Ireland	None (EEA) at the top level

Notes:

1. **Integrations the Customer connects are not Reditus Sub-processors.** Where the Customer connects its own HubSpot, User.com, Slack, Calendly or other account, or its own systems via the Reditus API and webhooks, that vendor is the Customer's processor: Reditus sends the data to the Customer's own account with a vendor the Customer chose.

2. **Google Ads and LinkedIn are independent controllers**, running on Reditus's own web properties for Reditus's own marketing; they are disclosed in the Reditus privacy notice, not here.

3. **Corporate vendors that never touch Customer Personal Data** (Reditus's own CRM, workspace and similar tooling, for which Reditus is the controller) are listed for transparency on the sub-processor page, not in this Annex.

End of the Reditus Data Processing Agreement, version 1.0 (concise edition), effective 4 August 2026. Reditus B.V., Kapelweg 12, 3951 AC Maarn, Netherlands, KvK 77814487, VAT NL861156420B01.