

Data Processing Addendum

Version 3.4 · online edition · 7 October 2026 · Melya Holding B.V., trading as HyperW

Entered into pursuant to Article 28 of Regulation (EU) 2016/679 (General Data Protection Regulation)

THE PARTIES

Processor	Melya Holding B.V., a private limited company incorporated under the laws of the Netherlands, having its registered office in Papendrecht, operating the HyperW service (the "Processor", "HyperW" or "we")
Customer	The legal entity that has entered into the Main Agreement for the HyperW service (the "Controller", "Customer" or "you")
Service	HyperW, a multi-tenant, AI-powered B2B website personalization engine accessible at app.hyperw.net and related endpoints
Contact	privacy@hyperw.net · hyperw.net/privacy
Document	Data Processing Addendum · Schedule 1 to the Main Agreement · version 3.4, online edition

This Data Processing Addendum ("DPA" or "Addendum") forms an integral part of, and is governed by, the SaaS Subscription Agreement or other master services agreement between the Processor and the Customer (the "Main Agreement"). In the event of any conflict between this DPA and the Main Agreement in respect of the Processing of Personal Data, this DPA prevails. In the event of any conflict between this DPA and the Standard Contractual Clauses referenced in Article 9, the Standard Contractual Clauses prevail.

The Parties have agreed as follows.

1. Definitions

1.1 Terms in capitals used but not defined in this DPA have the meaning given to them in the GDPR or in the Main Agreement.

1.2 In this DPA:

(a) "GDPR" means 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;

(b) "Applicable Data Protection Law" means the GDPR together with any national implementing or supplementary laws, including the Dutch Uitvoeringswet AVG (UAVG), and the EU ePrivacy rules as transposed into the Dutch Telecommunicatiewet, to the extent applicable to the Processing under this DPA;

(c) "Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Personal Data Breach" and "Supervisory Authority" have the meanings given in Article 4 GDPR;

(d) "Customer Personal Data" means Personal Data Processed by the Processor on behalf of the Customer under the Main Agreement, as further described in Annex 1;

(e) "Sub-processor" means any third party engaged by the Processor to Process Customer Personal Data on its behalf;

(f) "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission in Implementing Decision (EU) 2021/914;

(g) "Aggregated and Anonymised Data" means data derived from the Processing that has been irreversibly aggregated and stripped of all identifiers such that it no longer relates to an identified or identifiable natural person, as further described in Article 15.5.

2. Roles of the Parties and Subject Matter

2.1 The Customer is the Controller and the Processor is the Processor in respect of the Customer Personal Data, except where the Customer itself acts as a processor on behalf of a third-party controller, in which case the Processor acts as a sub-processor and the obligations in this DPA apply accordingly.

2.2 The subject matter, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are described in Annex 1. The Processor shall Process Customer Personal Data only for the purpose of providing the HyperW service under the Main Agreement and only on documented instructions from the Customer.

2.3 The Customer warrants that it has a valid legal basis under Article 6 GDPR for the Processing it instructs, that it has provided all required information to Data Subjects, and that its instructions comply with Applicable Data Protection Law.

3. Duration of the Processing

3.1 This DPA takes effect on the same date as the Main Agreement and remains in force for as long as the Processor Processes Customer Personal Data on behalf of the Customer.

3.2 The provisions that by their nature are intended to survive termination, including Articles 6 (Confidentiality), 11 (Personal Data Breach), 14 (Return and Deletion) and 15 (General), survive termination or expiry of this DPA and the Main Agreement.

4. Processing on Documented Instructions

4.1 The Processor shall Process Customer Personal Data only on documented instructions from the Customer, including with regard to transfers of Customer Personal Data to a third country, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

4.2 The Main Agreement, this DPA (including its Annexes), the configuration choices the Customer makes within the HyperW administration interface, and any further written instructions agreed between the Parties constitute the Customer's complete and documented instructions.

4.3 The Processor shall immediately inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. The Processor is not obliged to carry out an instruction it reasonably considers unlawful.

5. Obligations of the Processor

5.1 In addition to its other obligations under this DPA, the Processor shall:

- (a) Process Customer Personal Data only as set out in Article 4;
- (b) ensure that persons authorised to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) implement and maintain the technical and organisational measures described in Article 7 and Annex 2;
- (d) respect the conditions in Article 8 for engaging Sub-processors;
- (e) assist the Customer as set out in Articles 10, 11 and 12;
- (f) at the choice of the Customer, delete or return Customer Personal Data as set out in Article 14;
- (g) make available to the Customer the information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits as set out in Article 13.

5.2 The Processor shall ensure data minimisation by collecting only the Customer Personal Data necessary to deliver the service, and shall apply the retention limits described in Annex 1.

6. Confidentiality

6.1 The Processor shall keep Customer Personal Data confidential and shall not disclose it to any third party except as permitted by this DPA, required to provide the service, or required by law.

6.2 The Processor shall ensure that access to Customer Personal Data is limited to those personnel who require access to perform the Main Agreement, on a need-to-know basis, and that all such personnel are bound by binding confidentiality obligations.

7. Security of Processing

7.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

7.2 The measures implemented by the Processor are described in Annex 2. The Processor may update these measures from time to time provided that the level of security is not materially reduced.

7.3 Customer Personal Data is stored within the European Union: the primary data store operates in EU data centres (Upstash Redis, region eu-central-1, Frankfurt) and behavioural analytics run on EU infrastructure (PostHog EU). Requests are processed by the application layer hosted by Vercel: the serverless functions run in the Vercel region fra1 (Frankfurt, European Union), and the edge network that receives the visitor's request is global (the edge location that serves the visitor). Transfers to Sub-processors outside the European Economic Area are governed by Article 9 and Annex 3.

8. Sub-processors

8.1 The Customer provides general written authorisation for the Processor to engage Sub-processors. The Sub-processors engaged at the date of this DPA are listed in Annex 3.

8.2 The Processor shall inform the Customer of any intended addition or replacement of a Sub-processor at least fourteen (14) days in advance, thereby giving the Customer the opportunity to object on reasonable data-protection grounds. If the Customer objects and the Parties cannot reach a resolution, the Customer may terminate the affected part of the Main Agreement.

8.3 The Processor shall impose on each Sub-processor, by way of a written contract, data-protection obligations no less protective than those in this DPA. The Processor remains fully liable to the Customer for the performance of each Sub-processor's obligations.

9. International Transfers

9.1 The Processor shall not transfer Customer Personal Data to a country outside the European Economic Area unless it has taken measures to ensure the transfer is lawful under Chapter V GDPR.

9.2 Where a Sub-processor is located in, or Processes Customer Personal Data from, a third country that is not the subject of an adequacy decision, the transfer shall be governed by the Standard Contractual Clauses, which are incorporated into this DPA by reference and completed in accordance with Annex 3, supplemented by any additional safeguards required following a transfer impact assessment.

10. Assistance with Data Subject Rights

10.1 Taking into account the nature of the Processing, the Processor shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject rights laid down in Chapter III GDPR (including access, rectification, erasure, restriction, portability and objection).

10.2 Where a Data Subject submits a request directly to the Processor, the Processor shall promptly forward it to the Customer and shall not respond to the request itself except on the documented instructions of the Customer.

10.3 Customer Personal Data is held primarily in the Processor's Redis data store with all identifiers centralised, enabling deletion or export in response to a Data Subject request. Where Customer Personal Data has also been pushed to a Customer-controlled destination (for example the Customer's Microsoft Teams environment or its webhook endpoint), the Customer is responsible for fulfilling the request in those destinations.

11. Personal Data Breach

11.1 The Processor shall notify the Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

11.2 The notification shall, to the extent known, describe:

- (a) the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records concerned;
- (b) the likely consequences of the breach;

- (c) the measures taken or proposed to address the breach and to mitigate its possible adverse effects;
- (d) the name and contact details of a point of contact from whom more information can be obtained.

11.3 The Processor shall assist the Customer in meeting the Customer's own obligations to notify the Supervisory Authority and affected Data Subjects under Articles 33 and 34 GDPR. The Processor shall not notify any Supervisory Authority or Data Subject on the Customer's behalf unless legally required or instructed to do so by the Customer.

12. Data Protection Impact Assessment and Prior Consultation

12.1 The Processor shall provide reasonable assistance to the Customer with any data protection impact assessment and any prior consultation with a Supervisory Authority that the Customer is required to carry out under Articles 35 and 36 GDPR, taking into account the nature of the Processing and the information available to the Processor.

13. Audit Rights

13.1 The Processor shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

13.2 Audits shall be conducted on reasonable prior written notice of at least thirty (30) days, during normal business hours, no more than once per calendar year (save where required by a Supervisory Authority or following a Personal Data Breach), and in a manner that does not unreasonably disrupt the Processor's operations. The Processor may satisfy an audit request by providing relevant certifications, third-party audit reports or a completed security questionnaire where these reasonably address the Customer's request.

13.3 Each Party bears its own costs in connection with an audit, save that the Customer shall reimburse the Processor's reasonable costs for any audit that goes beyond the provision of existing documentation.

14. Return and Deletion of Personal Data

14.1 Upon termination or expiry of the Main Agreement, the Processor shall, at the choice of the Customer, delete or return all Customer Personal Data and delete existing copies, unless Union or Member State law requires storage of the Customer Personal Data.

14.2 The Customer may make such a request within thirty (30) days of termination. In the absence of a request, the Processor shall delete the Customer Personal Data within ninety (90) days of termination. Session-level data is in any event subject to a rolling thirty (30) day time-to-live and is deleted automatically thereafter.

14.3 Article 14.1 does not apply to Aggregated and Anonymised Data, which is not Personal Data and is dealt with under Article 15.5.

14.4 Alerts, notifications, reports and drafts that have already been delivered to a destination controlled by the Customer (such as the Customer's Microsoft Teams environment or its webhook endpoint) fall outside the Processor's control from the moment of delivery. Deletion under this Article does not extend to such delivered copies; their retention and deletion are governed by the Customer's own retention policy.

14.5 Back-ups. The Processor keeps two kinds of back-up:

(a) a daily snapshot of the entire primary data store (Upstash Redis), made by the database provider and including visitor data. Only the most recent snapshot is retained (retention of one day), so Customer Personal Data that has been erased or deleted from the primary data store is no longer present in any back-up within one day;

(b) snapshots taken by an authorised administrator of the Customer's configuration and content only (client configuration, knowledge base, brand material, playbook configuration, campaign articles, uploaded documents and domain mappings). Visitor data (sessions, identity, consent and content-fatigue records) is excluded from these snapshots.

15. General Provisions

15.1 Governing law and jurisdiction. This DPA is governed by the laws of the Netherlands. Any dispute arising out of or in connection with this DPA shall be submitted to the competent court in Rotterdam, without prejudice to the jurisdiction provisions of the Standard Contractual Clauses where these apply.

15.2 Liability. 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 Main Agreement, and any reference in the Main Agreement to a Party's liability means the aggregate liability of that Party under the Main Agreement and this DPA together.

15.3 Order of precedence. This DPA supplements and is incorporated into the Main Agreement as Schedule 1. Where the Main Agreement and this DPA conflict in respect of the Processing of Personal Data, this DPA prevails.

15.4 Novation to HyperW B.V. The Processor is currently Melya Holding B.V. The Parties acknowledge that the HyperW service is to be transferred to HyperW B.V. upon its incorporation. The Customer hereby consents in advance to the novation of this DPA and the Main Agreement from Melya Holding B.V. to HyperW B.V. upon such incorporation, with effect from the date HyperW B.V. notifies the Customer in writing of the transfer. All rights and obligations under this DPA continue unaffected following the novation.

15.5 Aggregated and Anonymised Data. The Processor may create Aggregated and Anonymised Data from the Processing and may use such data for the operation, improvement and benchmarking of the HyperW service, including cross-customer intelligence. Because Aggregated and Anonymised Data has been irreversibly stripped of all identifiers before aggregation and no longer relates to any identified or identifiable natural person, it falls outside the scope of the GDPR. The ownership of, and the Processor's rights in, such data are governed by the Main Agreement.

15.6 Changes. The Processor may update this DPA where required by changes in Applicable Data Protection Law, the addition of new safeguards, or changes to the service, provided that no such change materially reduces the protection of Customer Personal Data. Material changes will be notified to the Customer with at least thirty (30) days' notice.

15.7 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions continue in full force and the invalid provision is replaced by a valid provision that most closely reflects the original intent.

ACCEPTANCE

This online edition of the DPA applies where the Main Agreement is concluded through HyperW's online Signup under the HyperW Online Subscription Terms. For the purposes of this DPA, those Subscription Terms are the Main Agreement, and this DPA is Annex 1 to them; references in this DPA to "Schedule 1"

refer to that Annex 1.

The Customer accepts this DPA electronically at the Signup, together with the HyperW Online Subscription Terms, by ticking the dedicated box, which is not pre-ticked. No signature is required. The Processor records the version of this DPA that was accepted, the time of acceptance and the account through which it was accepted, and confirms the conclusion of the Main Agreement by e-mail. Where this DPA refers to the Order Form, for a Customer that signed up online that reference means the confirmation the Customer gives in the administration interface when it creates campaign links, including its declaration of the origin of the data and the legal basis it relies on. The text of this edition is otherwise identical to version 3.4 of the DPA used with signed agreements.

Annex 1: Details of the Processing

Subject matter of the Processing

Provision of the HyperW B2B website personalization service, under which visitor behaviour and contextual signals on the Customer's website are used to generate and serve personalized content and to surface lead-intelligence to the Customer.

Nature and purpose of the Processing

Collection, storage, organisation, analysis, enrichment and retrieval of visitor and contextual data for the purpose of (a) real-time content personalization; (b) lead identification and intent scoring; (c) generation of personalized panels using a third-party AI model; and (d) reporting and analytics for the Customer.

Device fingerprinting (FingerprintJS), the inference of the company from a business email address, role identification, and recognition across multiple visits (including the Identity Network look-up described below) take place exclusively after the visitor has provided consent via the consent banner managed by HyperW on behalf of the Customer (Art. 28(3)(a) GDPR). Without such consent, processing is limited to recognition at the organizational level based on IP address, in accordance with the balancing of interests determined by the Customer. Consent records are available to the Customer upon request as a JSON export.

Possible future processing (not available in the service at the date of this DPA). Conversion feedback to advertising platforms (such as LinkedIn), consisting of the transmission of a platform click identifier upon a conversion event, takes place only where the Customer has explicitly enabled it and only on the basis of a separate, specific consent scope obtained from the visitor and recorded in the consent registration. Absent such activation and consent, no data is transmitted to advertising platforms.

Identity Network. A visitor who has signed in with LinkedIn or Microsoft on a HyperW funnel may give a separate consent (consent scope "hyperw_network_v1") to be recognised on other sites. The Processor then keeps an Identity Network record keyed by the visitor's e-mail address, containing the e-mail address, name, company, job title, industry, the device fingerprints linked to it (with the source and HyperW customer of each link), the moment of consent, the last-seen date and the HyperW customers on whose funnels the consent was given, together with a pointer from each linked device fingerprint to the e-mail address. The record is not tied to one customer of the Processor. On the funnel of any HyperW customer, once the visitor has accepted that customer's consent banner, the visitor's device fingerprint is looked up in the Identity Network; on a match, the company and industry pre-fill the visitor's session. Recognition therefore works across the funnels of different HyperW customers. The e-mail address and name of a recognised visitor can appear in the Customer's alerts: in the alert for a known visitor returning through a mobile network, and in the "visitor identified" alert where the Customer has enabled that alert. The look-up runs only after the visitor has accepted the consent banner on the Customer's funnel; it does

not run for a visitor who declined or did not answer the banner. The separate network consent is currently requested only on the legacy funnel version; the look-up runs on every funnel. Retention is set out under "Duration of the Processing".

E-mail anchor and cross-customer visit record. When a visitor who has accepted the consent banner signs in with LinkedIn or Microsoft, or submits a business e-mail address through a form, the Processor keeps an e-mail anchor record (business e-mail address, company, industry, linked device fingerprints, first and last seen) that is not tied to one customer of the Processor; when that e-mail address is later supplied in a consented session on the funnel of any HyperW customer, the company and industry are pre-filled. For every visitor who has accepted the consent banner, the Processor also keeps a cross-customer visit record per device fingerprint (per HyperW customer visited: the industries shown, the highest intent score, the total number of visits, the last-seen date and the number of panels viewed). This cross-customer history is shown in a Customer's alerts only where the Processor has enabled it for that Customer's sales partner; it is off by default.

Optional campaign processing. Where the Customer creates campaign links and distributes them through its own channels (email, LinkedIn, or QR codes on the Customer's own material), each link may carry a signed token that identifies the campaign recipient. The token carries the recipient identifier supplied by the Customer, the campaign identifier and the channel. Upon a click on such a link, the Processor processes, to attribute the visit to the campaign recipient: the token, the click timestamp, the consent state, the approximate location derived from the IP address (country and city), and a classification of the click as a person or as an automated mail scanner. The Processor records clicks and visits per recipient, and sends the Customer a campaign-click or campaign-visit alert naming the recipient, the campaign, the channel and the approximate location; this click record and alert do not depend on the visitor's consent state. Only after the visitor has accepted the consent banner does the Processor place an anchor cookie on the visitor's device that holds the signed token, so that later visits in the same browser are attributed to the recipient. The token is removed from the page address before the page is delivered and is not disclosed to analytics Sub-processors. The Customer, as Controller, determines the legal basis for this processing and records it, together with the declaration required by the Processor, in the Order Form, to which the applicable balancing of interests is annexed; the Processor acts on the Customer's documented instructions. Retention is set out under "Duration of the Processing". Absent campaign links created by the Customer, no campaign tokens are processed.

Duration of the Processing

For the term of the Main Agreement. Return and deletion on termination is governed by Article 14. Within the term, the following retention periods apply:

Data	Retention
Session record keyed by device fingerprint	30 days after the last activity; the period restarts on every consented visit
Session record keyed by IP address, used where no device fingerprint is available (the full IP address is part of the record key)	30 days after the last activity; the period restarts on every consented visit
Content-fatigue counters (keyed by device fingerprint or IP address)	30 days from the first impression (default setting)
Session cookie on the visitor's device	14 days
Visitor-binding cookie on the visitor's device	30 days, renewed on every visit

Data	Retention
Consent records	2 years from the moment consent is given or withdrawn, serving as evidence of consent under Article 7(1) GDPR
Aggregated consent counters	90 days
Cookie storing the visitor's consent choice	180 days
Daily organisation-level visit statistics	90 days
Company-level intent records, the per-visitor identity record and the follow-up status per company	90 days after the last update
Cross-customer visit record (per device fingerprint)	90 days after the last activity
E-mail anchor record	365 days after the last update; not removed when consent is withdrawn on one customer's funnel; deleted upon an erasure request
Identity Network record and its device-fingerprint pointers	365 days after the last update; deleted upon an erasure request
Campaign link and its token	the validity chosen by the Customer when creating the link: 30 days by default, at most 365 days; links for LinkedIn posts and ABM links 90 days
Campaign anchor cookie on the visitor's device	until the token expires
Campaign click records	90 days
Campaign visit records	90 days after the last visit
IP lookup cache (full IP address with the organisation lookup result)	60 seconds
Hashed IP address used to detect automated mail scanners	15 minutes (landing) and 4 hours (verdict)
Engine diagnostic traces (only while diagnostics are enabled for the Customer)	14 days
Erasure confirmation link	1 hour
Daily snapshot of the primary data store (Article 14.5(a))	the most recent snapshot only (one day)
Operator labels that mark a device as test or internal traffic	365 days

Withdrawal of consent on the Customer's funnel deletes the session records, content-fatigue counters and per-visitor identity record of that browser for the Customer, and the Customer's entry in the cross-customer visit record. An erasure request confirmed through the e-mail link additionally deletes the e-mail anchor record and the Identity Network record.

Categories of Data Subjects

Visitors to the Customer's website, including prospective customers, business contacts and representatives of organisations browsing the Customer's site.

Types of Personal Data

Category	Examples
Network identifiers	IP address (also used as the key of the session record where no device fingerprint is available); approximate geolocation derived from IP (city / region / country)
Device / browser data	Browser and device fingerprint, user-agent, returning-visitor signal
Organisational data	Company / organisation name and inferred industry derived from IP, reverse-DNS and ASN lookups
Behavioural data	Page views, scroll and click events, content interactions, session references
Derived data	Intent score, visitor cohort, content-fatigue signal and other derived classifications
Optional contact data	Where the visitor submits it (e.g. business email address via a form), and the company inferred from the domain of that address
Optional campaign link data	Where the Customer creates campaign links: signed per-recipient token from links the Customer distributes itself, comprising the recipient identifier supplied by the Customer, the campaign identifier and the channel (email, LinkedIn, QR); click timestamp, consent state and approximate location (country, city); anchor cookie holding the token after consent
Sign-in profile data	Where the visitor signs in with LinkedIn or Microsoft: name, e-mail address, job title and company as returned by the sign-in provider
Identity Network and e-mail anchor data	E-mail address, name, company, job title, industry and linked device fingerprints, as described under "Identity Network" and "E-mail anchor and cross-customer visit record"

No special categories of personal data (Article 9 GDPR) are intentionally Processed. The Customer shall not configure the service to collect special category data.

Annex 2: Technical and Organisational Measures

The Processor implements and maintains the following measures in accordance with Article 32 GDPR. These measures may be updated provided the overall level of security is not materially reduced.

Data residency and segregation

Customer Personal Data is stored within the European Union and requests are processed by serverless functions in the Vercel region fra1 (Frankfurt, European Union), as set out in Article 7.3 and Annex 3. The multi-tenant architecture enforces tenant isolation: each tenant's data is namespaced by a unique client identifier and the API layer restricts access so that one tenant cannot access another tenant's data.

Encryption

Data is encrypted in transit using TLS. Secrets and API tokens are stored as encrypted environment variables and are not exposed to clients. The Customer's Microsoft Teams webhook URLs are stored encrypted at application level (AES-256-GCM).

Access control

Access to production systems and Customer Personal Data is restricted on a least-privilege, need-to-know basis. Administrative access is authenticated; cookies carry secure flags; session data is held with strict time-to-live limits.

Data minimisation and retention

The service collects only the data necessary for personalization and lead intelligence. Personal identifiers are centralised in a single store to enable controlled deletion. Session-level data carries a rolling 30-day time-to-live.

Logging and monitoring

Application errors and security events are monitored. Behavioural analytics are processed through EU analytics infrastructure and segmented by tenant.

Resilience and availability

The service runs on managed, redundant cloud infrastructure with automated deployment controls and environment separation between development and production.

Sub-processor governance

Sub-processors are bound by written contracts imposing data-protection obligations no less protective than this DPA, and are listed and maintained in Annex 3.

Breach management

Documented procedures are in place to detect, assess and notify Personal Data Breaches in accordance with Article 11 of this DPA.

Annex 3: Authorised Sub-processors

The following Sub-processors are authorised at the date of this DPA. The current list is maintained and made available to the Customer on request. Transfers outside the EEA, where they occur, are governed by the Standard Contractual Clauses and supplementary safeguards.

Sub-processor	Purpose	Location / Transfer basis
Vercel	Application hosting, edge network and serverless functions	Serverless functions in region fra1 (Frankfurt, EU); edge network global (the edge location serving the visitor); SCCs for any processing outside the EEA

Sub-processor	Purpose	Location / Transfer basis
Upstash (Redis)	Primary data store for session and visitor data	EU (eu-central-1, Frankfurt)
PostHog EU	Behavioural / product analytics; operates in cookieless mode and stores nothing on visitor devices; the request IP address is technically visible to this Sub-processor at ingestion and is not persistently stored	EU
IPInfo	IP geolocation lookup	SCCs where applicable
FingerprintJS	Device / browser fingerprinting and returning-visitor detection	SCCs where applicable
Anthropic (Claude API)	AI generation of personalized content	SCCs where applicable
Brandfetch	Organisation inference from the domain of a business e-mail address the visitor provides (legacy funnel version only; the request is made from the visitor's browser)	SCCs where applicable
Sentry	Error and performance monitoring	SCCs where applicable
Microsoft (Teams, via Power Automate webhooks)	Lead and operational alerting to the Customer where the Customer selects Microsoft Teams as its alert channel	Delivery into the Customer's own Microsoft 365 environment; SCCs where applicable
Google (Google Public DNS, DNS-over-HTTPS)	Reverse-DNS (PTR) lookup of the visitor's IPv4 address to determine the visiting organisation, on page requests before consent; MX lookup of the domain of a business e-mail address the visitor provides. The lookups are made from the Processor's servers; the visitor's IPv4 address is part of the PTR query	SCCs where applicable
Resend	Transactional e-mail, including the confirmation e-mail sent to a visitor who requests erasure, and service e-mails to the Customer	EU region (sending domain); SCCs where applicable
Upstash (QStash)	Message queue for the delayed processing of campaign-link clicks (token, consent state, country and city, click time) and for internal cache-warming jobs	EU

Where the Customer selects a destination it controls for alerts (such as its own Microsoft Teams environment or its webhook endpoint), that destination is not a Sub-processor of the Processor and the Customer acts as Controller in respect of that onward Processing.

Sign-in providers chosen by the visitor (LinkedIn, Microsoft Entra ID) are not Sub-processors: the visitor signs in with them directly, and they return the visitor's profile data to the service as independent recipients.

End of Data Processing Addendum