

DATA PROCESSING AGREEMENT

Version 1.0 · in force from August 23, 2026

This agreement forms part of the [Terms of Service](#) and applies whenever **EVA DAVA EOOD**, UIC 207945177, 9 Gen. Gurko Str., floor 1, 8000, Burgas, Bulgaria (the **Processor**), processes personal data on the instructions of a client (the **Controller**). It is entered into under Article 28(3) of Regulation (EU) 2016/679.

1 Roles

THE ALLOCATION, IN ONE LINE

For the campaign data, the Controller is the client and the Processor is EVA DAVA EOOD. The Controller decides who is contacted and why. The Processor carries that decision out.

The Controller's decision is not implied, it is documented: the buyer profile, the qualification criteria, the seniority, the geography, the messaging and the exclusion list are signed off by the Controller in writing before the first message is sent, under clause 11 of the [Terms of Service](#). Those documents are the instruction.

ACTIVITY	EVA DAVA ACTS AS
Sourcing and selecting prospects against the Controller's signed-off buyer profile	Processor
Verifying that a business address is deliverable before sending to it	Processor
Sending outbound from the Controller's domain and mailbox	Processor
Handling replies received in the Controller's mailbox	Processor
Writing contacts, notes, meeting records and opt-outs into the Controller's CRM	Processor
Booking meetings into the Controller's calendar	Processor
Keeping the permanent suppression list of people who asked never to be contacted again	Independent controller

The last row is the only exception and it is deliberate. A suppression list tied to one Controller would be deleted at the end of that engagement, and the same person would be contacted again for the next client. Keeping it separately, across all clients and beyond the end of any engagement, is the only way an objection can be

permanent. EVA DAVA answers for it as a controller under its [Privacy Notice](#), holds nothing in it beyond the address, the date and the fact of the request, and uses it for nothing but honouring the objection.

The Controller confirms that it has a lawful basis for the outbound activity it instructs. The balancing assessment under Article 6(1)(f) that supports it is set out in section 6 of the [Privacy Notice](#), is repeated for the Controller's own profile, and is supplied to the Controller on request so that the Controller can rely on it and defend it.

2 Subject matter and duration

Subject matter: identifying, contacting and qualifying business prospects, and booking meetings, on behalf of the Controller.

Duration: for as long as the engagement under the Terms of Service continues, and thereafter for the return or deletion period in clause 14.

3 Nature and purpose of processing

Collection, organisation, structuring, storage, use, transmission, restriction and erasure.

Purpose: identifying, contacting and qualifying business prospects within the buyer profile the Controller has signed off, and booking meetings with those who agree to one. There is no other purpose. Personal data processed for one Controller is never used for another, and the Controller's lists, copy, hook and angle are never reused.

4 Categories of data subject

Employees, officers and representatives of companies falling inside the agreed buyer profile, and people who reply to a message sent under the Service.

5 Categories of personal data

- name and job title;
- employer, business address and public company information;
- business email address;
- the content of replies;
- meeting records: time, attendance and notes on fit.

No special categories of data under Article 9 are processed, and none may be introduced without a written amendment to this agreement. No data relating to children is processed. No personal email addresses are used. There is no automated decision-making within the meaning of Article 22 and no profiling that produces legal or similarly significant effects.

6 Instructions

The Processor processes personal data only on the documented instructions of the Controller. The documented instructions are:

- the signed-off buyer profile and qualification criteria;
- the approved messaging and sequence;
- the exclusion list, and any addition to it;
- the volume ceiling;
- the retention instruction under clause 14;
- the Terms of Service and this agreement.

Where Union or Bulgarian law requires the Processor to process beyond those instructions, it informs the Controller before processing unless that law prohibits it.

The Processor informs the Controller if, in its opinion, an instruction infringes the GDPR, and does not carry it out until the point is resolved. This applies in particular to a request to send to a category the Processor excludes under clause 14 of the Terms of Service, and to a request to remove or weaken the opt-out mechanism in an outbound message.

7 Confidentiality

The Service is delivered by Alex Kuguk, the sole owner of the Processor, together with the crew he engages and directs, each of them bound by the confidentiality clause of the Terms of Service (clause 20).

Any further person given access to the Controller's data is bound by an equivalent written confidentiality obligation **before** access is granted, and access is granted only to what that person's part of the work requires.

8 Sub-processors

The Controller gives general written authorisation for the following sub-processors.

SUB-PROCESSOR	PURPOSE	LOCATION
Google Ireland Limited	Google Workspace: mailboxes on the Controller's domains, calendar, meetings, documents	EU, transfers to the US
Microsoft Ireland Operations Limited	Microsoft 365 and Exchange Online: the second half of the mailbox pack	EU, transfers to the US
Domain registrar and DNS	Registration of the Controller's domains, DNS and network	United States, with EU edge
Website host	Hosting of the public website and its server logs	United States
Prospect data provider (<i>named in writing before the engagement starts</i>)	Business contact data and outbound sequencing	United States
Email verification provider (<i>named in writing before the engagement starts</i>)	Deliverability check on a business address before sending	Outside the EEA, under SCCs

Both mailbox vendors are used on every engagement, by design: the pack is split across Google and Microsoft so that neither of them can take all of it out with a single suspension. That is an operating rule under clause 12 of the Terms of Service and it is also why both appear here.

The Processor gives the Controller **thirty days** written notice before adding or replacing a sub-processor. The Controller may object on reasonable data-protection grounds, and if the objection cannot be resolved either party may terminate the affected part of the Service without penalty.

Each sub-processor is engaged under a written contract imposing the same obligations as this agreement. **The Processor remains fully liable to the Controller for the performance of its sub-processors.**

9 Security

Measures appropriate to the risk under Article 32:

- **Access is per Controller and minimal.** The mailboxes on that Controller's domains, one CRM seat, and one nominated calendar. Nothing else, and no access to any other part of the Controller's systems;
- **Access is delegated, not shared.** The Controller revokes any of it in under a minute, at any time, without changing a password and without notice;
- two-factor authentication on every account used to deliver the Service;
- **Separation between clients.** One domain carries one mailbox, and five mailboxes sit in one tenant. A Controller's mailboxes are not mixed with another Controller's, so a compromise or a suspension is contained to one Controller and, within that, to one tenant;
- the Controller's existing contact records stay in the Controller's own systems and are not exported;

- encryption in transit throughout, and encryption at rest by the platforms named in clause 8;
- full-disk encryption on the operator's device;
- credentials held in an encrypted store, never in plain text and never inside the messaging tools;
- SPF, DKIM and DMARC set and verified on every domain before it sends, which is a security measure as much as a deliverability one: it is what stops a third party sending in the Controller's name;
- bounce and complaint monitoring with automatic stops at 2% and 0.1%, which limits the blast radius of a bad list.

10 International transfers

Transfers outside the European Economic Area rely on the European Commission's Standard Contractual Clauses (Decision 2021/914), and on the EU-US Data Privacy Framework where the recipient is certified under it. A transfer impact assessment is available to the Controller on request.

The email verification provider operates from a country that is not covered by an adequacy decision, so that transfer rests on the Standard Contractual Clauses alone. The country and the provider are named in writing before the engagement starts, and a transfer impact assessment for that recipient is held by the Processor and provided to the Controller on request. Only a business email address is sent, and no other personal data leaves the EEA for this purpose.

The Processor does not transfer the Controller's personal data to any country or recipient outside those arrangements without the Controller's written instruction.

11 Assistance to the Controller

Taking into account the nature of the processing and the information available to it, the Processor assists the Controller with:

- **Data subject requests under Articles 12 to 23.** A request received directly by the Processor is forwarded to the Controller **without undue delay and within two business days**, and is not answered by the Processor unless the Controller instructs it. The data subject is told who the controller is;
- **Objections to direct marketing under Article 21.** These are not held for an instruction. An objection or an opt-out is actioned **the same business day** by suppressing the address, is written into the Controller's CRM against the contact record, and the Controller is informed. This is the one action the Processor takes without waiting, because Article 21(3) does not permit a delay;
- **Security, breach notification, data protection impact assessments and prior consultation** under Articles 32 to 36, including supplying the balancing assessment and the record of processing for the Controller's campaign;
- demonstrating compliance, by supplying the sending records, the exclusion list as applied, and the suppression record for any address the Controller asks about.

12 Personal data breach

The Processor notifies the Controller **without undue delay and in any event within 24 hours** of becoming aware of a personal data breach affecting the Controller's data.

The notification carries the facts known at that time: what happened, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point. Further information follows as it becomes known, without waiting for a complete picture, so that the Controller can meet its own 72-hour duty under Article 33.

13 Audit

The Processor makes available the information needed to demonstrate compliance with Article 28, and allows for and contributes to audits by the Controller or an auditor it mandates.

- on fourteen days written notice, once per year, during business hours;
- more often where a supervisory authority requires it, or after a personal data breach affecting the Controller's data;
- the auditor is bound by confidentiality and is not a competitor of the Processor;
- the audit does not extend to another controller's data, and access to shared infrastructure is given in a way that does not expose it.

14 Return and deletion

During the engagement, the Processor retains prospect records for the period the Controller instructs. Where the Controller gives no instruction, the default is twelve months from the last contact, unless a conversation is still running, and it is recorded in the agreement either way.

On termination of the Service, at the Controller's choice, the Processor **returns or deletes** the personal data it holds and deletes existing copies, within **thirty days**. Written confirmation follows.

Two exceptions, both stated plainly rather than left in a schedule:

- **Suppression records are kept.** An address that asked never to be contacted again has to stay on the suppression list, or the objection cannot be honoured. Only the minimum needed for that purpose is retained: the address, the date, and the fact of the request. Nothing about the campaign, the message or the employer stays with it;
- data that Union or Bulgarian law requires to be retained, for the period that law requires and for no other purpose.

Data held in the Controller's own systems is not affected by any of this. It never left them.

15 Infrastructure after the end

The domains and the mailboxes are registered to the Controller's legal entity and remain the Controller's property when the engagement ends, under clause 9 of the Terms of Service.

This matters here and not only in the commercial terms: the mail, the sent history and the replies sit in accounts the Controller owns and controls. On termination the Processor's access is revoked and the data stays exactly where it was, with the Controller, without a migration and without a copy having to be handed over. There is no lock-in of the data because there was never custody of it in the first place.

16 **Liability and law**

Liability under this agreement is subject to the limitations in the Terms of Service, except where the GDPR does not permit limitation.

Where this agreement and the Terms of Service conflict on the processing of personal data, this agreement prevails. This agreement is governed by the law of the Republic of Bulgaria.

SIGNATURE

This agreement is accepted together with the Terms of Service and requires no separate signature. A countersigned copy on the Controller's own paper is provided on request: write to alex.kuguk@evadava.com.