Mimir Technologies

ENGINEERING FOR TEAMS THAT SELL

// SALES SIGNAL · UNITED STATES

Data Processing Agreement

Service provider terms for the personal information in the Company's leads

Version SS-DPA-US-2 | Version date October 18, 2026 | Signed together with the mutual NDA

01 Parties and roles

1.1 Parties. This agreement is between the company named on the acceptance page ("the Company") and Mimir Technologies SRL, a company registered in the Republic of Moldova under IDNO 1024600004597, str. Salcâmilor 5, Stăuceni, mun. Chișinău, Republic of Moldova ("Mimir").

1.2 Roles. For the personal information in the Company's leads, the Company is the business (or controller) and Mimir is its service provider (or processor), as those terms are used in the California Consumer Privacy Act as amended ("CCPA") and the other US state privacy laws that apply to the Company (together, "Privacy Laws"). Mimir processes that information only on the Company's behalf and only to deliver the Sales Signal ("the Business Purpose").

1.3 Signing. Mimir has signed this version in advance with an electronic signature applied to this file, which Adobe Acrobat Reader and other PDF readers that check signatures can verify. The Company signs by completing the acceptance page in the Sales Signal form, together with the Mutual Non-Disclosure Agreement (version SS-NDA-US-2, "the NDA"). The parties agree to do business electronically, and each signature is valid under the federal Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Uniform Electronic Transactions Act as adopted in Delaware and the other states that have adopted it. The agreement takes effect when the Company signs.

1.4 Order of documents. On anything about personal information, this agreement prevails over the NDA and the Terms of Use.

02 Mimir's commitments as service provider

Mimir will:

1. process personal information only for the Business Purpose and on the Company's documented instructions, which are this agreement and Annex 1;
2. not sell or share the personal information, as "sell" and "share" are defined in the CCPA;
3. not retain, use or disclose it for any purpose other than the Business Purpose, or outside the direct business relationship between the parties;

4. not combine it with personal information Mimir receives from anyone else, or collects itself, except as the Privacy Laws permit;
5. comply with the obligations that apply to it under the Privacy Laws, and give the personal information the same level of privacy protection those laws require of the Company;
6. tell the Company promptly, and within 5 business days, if it can no longer meet these obligations;
7. let the Company take reasonable and appropriate steps to ensure Mimir uses the information consistently with the Company's obligations, and to stop and remediate any unauthorized use;
8. bind every person who processes the information to confidentiality — today one named analyst;
9. help the Company respond to consumers' requests to know, delete or correct their information, passing any request it receives to the Company within 3 business days rather than answering it;
10. give the Company the information it reasonably needs to show compliance and to carry out any risk or data protection assessment the Privacy Laws require;
11. bind each subcontractor listed in Annex 3 by a written contract with the same obligations, and give the Company 14 days' notice by email before adding or replacing one, so that it can object. If the Company objects on reasonable grounds, Mimir does not use the new subcontractor for the Company's information or, if it cannot avoid doing so, the Company may end this agreement and Mimir deletes the information under clause 5.2.

Mimir certifies that it understands and will comply with these restrictions.

03 Access, processing and location

3.1 Read-only access. The Company gives Mimir temporary read-only access to its CRM, by a read-only API key or a read-only user. The access must allow viewing only: no creating, editing or deleting records, no bulk-export functions and no sending messages. Mimir refuses a key that can write, wherever the CRM shows a key's permissions.

3.2 Scope and use. Mimir reads only the last 30 days of leads in the agreed pipeline, and the Company's price list, catalogue and sales rules; nothing else. A key is used only by Mimir's software; a read-only user only by one named analyst with two-factor authentication, or by Mimir's software acting as that user, within the CRM's request limits. Keys are encrypted in the Company's browser before they are sent, and never travel by email. Mimir never messages the Company's customers or changes anything in the CRM.

3.3 End of access. Access ends 7 days after the findings call, or, if no call takes place, 7 days after the Sales Signal is canceled or this agreement ends, unless the Company continues under a separate agreement. Mimir deletes any stored key, reminds the Company to revoke the access, and confirms in writing.

3.4 Recordings and AI. Recordings are transcribed on Mimir's servers, hosted by Hetzner in Germany. Before any text leaves those servers, a redaction engine replaces names, phone numbers, emails, addresses, dates of birth, ID, card and account numbers with placeholders. No automatic redaction catches everything, so Mimir checks samples by hand and protects redacted text as personal information. Redacted text is analyzed through Amazon Bedrock with no data retained by Amazon and no model training. Mimir never uses the Company's data to train any model, never infers emotions from anyone's voice, and never recommends disciplinary action. Every finding cites its source, and a person checks it before the Company sees it.

3.5 Where data is kept. Personal information is stored and processed on Mimir's servers in Germany. Automatically redacted text is analyzed in the United States through Amazon Bedrock. Emails with the Company and the findings call go through the providers listed in Annex 3. Mimir's team accesses the information from the Republic of Moldova. The Company agrees to this processing outside the United States. Neither Germany nor Moldova is a "country of concern" under the US Department of Justice rule on access to bulk sensitive data (28 CFR Part 202), and Mimir gives no person from such a country access.

04 Regulated data

4.1 No health information. The Sales Signal is not designed for protected health information under HIPAA. The Company will not give Mimir access to protected health information, and confirms that the agreed pipeline contains none, unless the parties first sign a separate business associate agreement. If Mimir finds such information, it stops processing that lead, tells the Company, and deletes it.

4.2 Insurance and financial companies. Where the Company is a financial institution under the Gramm-Leach-Bliley Act, or is subject to a state insurance data security law, Mimir maintains the safeguards in Annex 2, which are designed to protect the security and confidentiality of customer information, and cooperates with the Company's oversight of its service providers.

4.3 Call recording consent. Federal and state laws govern recording calls, and some states require every party's consent. The Company confirms that the recordings it makes available were made lawfully, with any notice and consent those laws require, and that its employees have been told their conversations may be reviewed, including by outside providers, to improve the quality of sales.

4.4 Sensitive information. Subject to clause 4.1, the Sales Signal does not aim to process sensitive personal information such as health information, financial account numbers or government ID numbers. Where such data appears, it is redacted where the engine finds it, never used for a finding about the customer, and deleted with the rest.

4.5 Indemnity. The Company will defend and indemnify Mimir against third-party claims, regulatory fines (to the extent the law allows them to be indemnified) and reasonable legal costs arising from recordings made without the notice or consent the law requires, or from personal information the Company had no right to make available. Mimir will defend and indemnify the Company against third-party claims, regulatory fines (to the extent the law allows them to be indemnified) and reasonable legal costs arising from Mimir's breach of this agreement. The party claiming tells the other promptly, lets it control the defense and any settlement, and cooperates at the indemnifying party's cost. The indemnifying party may not agree to a settlement that admits fault for, or places obligations on, the other party without its consent. Indemnities fall within the limit in clause 5.5.

05 Incidents, deletion and legal terms

5.1 Security incidents. Mimir notifies the Company without undue delay, and within 48 hours, after discovering unauthorized access to or acquisition of the Company's personal information. It gives what it knows as it learns it, takes reasonable steps to contain the incident, and helps the Company meet any breach notification duty under state law. Mimir does not notify consumers or regulators on the Company's behalf without its instruction, unless the law requires it.

5.2 Deletion. Within 7 days of the findings call, or, if no call takes place, within 7 days after the Sales Signal is canceled or this agreement ends, Mimir deletes, or at the Company's written choice returns and then deletes, all personal information it holds for the Sales Signal — recordings, transcripts, messages, CRM data, redacted text, the redaction key and its own copy of the findings — and certifies the deletion in writing. Recordings are deleted earlier, once transcribed and checked. Copies in encrypted backups expire within 30 days and are never restored for use in the meantime. The deletion does not cover the signed agreements, the signing record and emails exchanged with the Company, which Mimir keeps as its Privacy Notice describes, except personal information about the Company's leads or customers in those emails, which is deleted with the rest.

5.3 Audits. Mimir answers the Company's reasonable written questions about its compliance within 14 days. If that is not enough, the Company, or an independent auditor bound by confidentiality, may audit once a year, on 30 days' notice, at the Company's cost.

5.4 The Company's duties. The Company confirms that it has the right to make the personal information available for the Business Purpose, and that it has given any notice to consumers and employees that the Privacy Laws require.

5.5 Liability. NEITHER PARTY IS LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS. EACH PARTY'S TOTAL LIABILITY UNDER THIS AGREEMENT, HOWEVER IT ARISES, IS LIMITED TO US$25,000. NEITHER LIMIT APPLIES TO BREACH CAUSED BY WILLFUL MISCONDUCT OR GROSS NEGLIGENCE.

5.6 Term. This agreement runs from signing until Mimir has deleted all personal information under clause 5.2. Clauses 2(8), 4.5, 5.2, 5.5 and 5.7 survive.

5.7 Law, forum and notices. Governing law and forum are the same as in the mutual NDA (clause 4.5). Notices go by email: to Mimir at cristian.rusu@mimir.md, and to the Company at the signer's email.

ANNEX 1 Processing details

Business Purpose	Preparing and delivering the Sales Signal: three findings about how the Company's leads were worked, what was offered and how conversations went, walked through on a findings call
People concerned	The Company's leads and customers; its employees who handle them
Information	Names and contact details; content of calls, messages and chats; call recordings; CRM records and activity; the employee assigned to each lead
Scope	The last 30 days of leads in the agreed pipeline, and the Company's price list, catalogue and sales rules; nothing else
Duration	Until deletion, 7 days after the findings call (or after cancellation, if no call takes place); encrypted backups expire within 30 days

ANNEX 2 Security measures

Servers in ISO/IEC 27001-certified data centers in Germany (Hetzner's certificate, not Mimir's); encryption in transit and at rest with keys held apart, with data decrypted only in memory while it is transcribed or redacted; keys to the CRM encrypted in the browser; automatic redaction before any text leaves Mimir's servers, checked by hand on samples; access limited to one named analyst with two-factor authentication, and every access logged; servers and software kept up to date with security patches; a written incident response procedure; read-only, 30-day, one-pipeline scope; deletion within 7 days with written confirmation; incident notice within 48 hours. Mimir holds no SOC 2 or ISO 27001 certification and does not claim to.

ANNEX 3 Subcontractors

COMPANY	WHAT IT DOES	WHERE	INFORMATION IT SEES
Hetzner Online GmbH	Servers: storage, transcription, redaction	Germany	All; encrypted at rest, decrypted only in memory while processed
Amazon Web Services (Amazon Bedrock)	Analysis of redacted text	United States	Automatically redacted text only; nothing retained
Google (Google Workspace)	Email with the Company, and the findings call over Google Meet; calls are never recorded	United States and other countries where Google operates	Only what is written in emails or shown on the call
Microsoft (Microsoft 365)	Email with the Company, where it goes through our Microsoft mailboxes	United States and other countries where Microsoft operates	Only what is written in emails

Signatures

SIGNED IN ADVANCE

FOR Mimir Technologies SRL

NAME

Cristian Rusu

TITLE

Administrator

SIGNATURE

Electronic signature on this file, version SS-DPA-US-2. Verify it in the PDF's signature panel

DATE

October 18, 2026

FOR the Company

LEGAL COMPANY NAME

STATE OF INCORPORATION

PRINCIPAL BUSINESS ADDRESS

SIGNED BY (NAME)

TITLE

SIGNATURE (TYPED NAME)

SIGNED ON

☐ The signer confirms they are authorized to sign for the Company

The Company signs on the acceptance page of the Sales Signal form. Its signing record — date and time, email, IP address and the fingerprint of this signed file — is issued to both parties as an acceptance certificate, with this file attached unchanged.