Mimir Technologies

ENGINEERING FOR TEAMS THAT SELL

// SALES SIGNAL · UNITED STATES

Privacy Notice

How we handle personal information from our website, the Sales Signal form, booked calls and our emails

Version PN-US-2 | United States edition | Last updated October 18, 2026

Who we are and what this covers

Mimir Technologies SRL ("we") is responsible for the personal information described here. This notice covers people in the United States who visit mimir.md/sales-review, fill out the Sales Signal form, sign our NDA and DPA, book a call with us, or receive an email from us.

Company	Mimir Technologies SRL, IDNO 1024600004597
Address	str. Salcâmilor 5, Stăuceni, mun. Chișinău, Republic of Moldova
Contact for anything in this notice	cristian.rusu@mimir.md · +373 68 939 111

What this notice does not cover. When a company gives us access to its CRM, we read its leads' calls and messages on that company's behalf. For that information the company is the business and we are its service provider, under the Data Processing Agreement we sign with it. How we handle it is set out in that agreement and on our Your data page. If you are a customer or employee of one of our clients, the client is who you contact first.

What we collect, why, and for how long

We collect only what we need to answer you, write to people our service may be relevant to, prepare a Sales Signal and prove what was agreed. We don't sell it, and we don't use it for targeted or cross-context behavioral advertising.

WHAT	WHERE IT COMES FROM	WHY	HOW LONG WE KEEP IT
Website visits: IP address, browser, pages requested, time	Your browser, in our server logs	To keep the site running and secure	30 days
The Sales Signal form: name, work email, company, role, team size, lead volume, what you record, your CRM, and anything optional you add (phone, conversion rate, gross profit per customer)	You	To answer your request and prepare your Sales Signal	12 months from our last contact if no agreement follows; otherwise as for the signing record
The signing record: your name, title, typed signature, email, company details, the time, your IP address, and the versions of the documents you signed with their fingerprints	You and your browser	To prove who agreed to what, and when	The length of the signed agreements plus 3 years
Access to your CRM: the read-only key, or the login of the user you create for us	You or your CRM admin	To read your leads under the DPA	Deleted or deactivated at most 7 days after the findings call, unless we continue under a separate signed agreement
Booked calls: name, email, the time you chose, anything you write in the booking	You, through our booking page	To hold the call over Google Meet. We never record calls	12 months from the call
Emails between us	You	To reply and keep track of the conversation	24 months from our last contact
Outreach emails we send	See the next section		

The form makes one automatic check: it looks at team size and whether calls or messages are recorded, and tells you straight away if a Sales Signal isn't a fit yet. It decides nothing else about you, and you can always write to us instead.

· If we emailed you first

We write to people whose role makes our service relevant to them — usually sales, commercial or operations leaders at companies with larger sales teams. We write to work addresses only, a few times at most, and every email says how to stop.

- **What we hold:** your name, work email, job title, company, and your company's state and industry; whether our email was delivered, opened or replied to, and whether you asked us to stop.
- **Where we got it:** your company's website, public business registers, and Apollo.io. We check that the address exists with MillionVerifier before we write.
- **How we use it:** to offer you a service relevant to your work. An AI tool reads your company's public website to help us judge whether our service is likely to be relevant and to write one line about your company. It reads public company pages, together with your name and job title; it is not used to decide anything else about you.
- **How to stop:** reply "stop", or write to cristian.rusu@mimir.md. We stop for good, usually the same day and at the latest within 10 business days. We keep only your email address on a do-not-contact list, so that we never write again. We never sell your address or give it to anyone other than the service providers listed below.
- **Our emails:** every email says who we are, makes clear it is a business offer, gives our postal address and includes a way to stop.
- **How long:** 12 months from our last email if you don't reply. The do-not-contact entry stays for as long as we send emails.

Who else receives it, and where it is kept

We share personal information only with the service providers that run our work, each bound by contract to use it only for us, and otherwise only where the law requires, to protect our legal rights, or with a successor of our business.

COMPANY	WHAT IT DOES FOR US	WHERE
Hetzner Online GmbH	Our servers: the site, the form, our booking calendar and signing records	Germany
Google (Google Workspace)	Our mailboxes, call invitations, video calls over Google Meet, and internal team alerts	United States and other countries where Google operates
Microsoft (Microsoft 365)	Our mailboxes	United States and other countries where Microsoft operates
Apollo.io (ZenLeads Inc.)	Finding work contact details for our outreach	United States
MillionVerifier (GBD Software as a Service Private Limited Company)	Checking that an email address exists before we write; uploaded lists are deleted within 30 days	Hungary, and other countries per its own list of providers
Anthropic PBC	The AI tool that reads companies' public websites for our outreach	United States

Where it is kept. Our servers are in Germany. Our outreach records — the companies and people we write to, and what happened to each email — are kept on an encrypted computer we run ourselves in the Republic of Moldova, where our team works. Your information is therefore stored and handled outside the United States.

Backups. Our servers are backed up in encrypted form, and backups expire within 30 days. Information we delete disappears from them within that time.

Security. Information is encrypted in transit and at rest. Keys to your CRM are encrypted in your browser with our public key before they are sent. Our servers store them only in that encrypted form and never hold the private key; we decrypt a key offline, on a computer kept separate from our servers. Only the people who need it can open your information, with two-factor authentication.

Your rights

Several US states, including California, Virginia, Colorado, Connecticut and Texas, give their residents rights over their personal information. We give these rights to everyone, whichever state you live in. You can ask us to:

- tell you what personal information we hold about you, where it came from, why we use it and who receives it, and send you a copy;
- correct it;
- delete it, unless we must keep it to prove an agreement, or keep your address on our do-not-contact list;
- stop emailing you — this one always applies, with no reason needed.

How to ask. Write to cristian.rusu@mimir.md from the address concerned, or tell us which address it is. We may ask for a detail or two to confirm it is you, and never more than we need. Someone you authorize may ask for you, with your written permission. We confirm your request within 10 business days and answer within 45 days; if we need up to 45 more, we tell you why.

Appeals. If we decline a request, you can appeal by replying to our answer, and we answer the appeal within 45 days. If you still disagree, you can contact your state's attorney general.

No discrimination. We never treat you differently for using these rights.

No selling or sharing. We do not sell or share personal information, as those terms are used in California law, and we do not use it for targeted advertising, so there is nothing to opt out of. We still treat a Global Privacy Control signal from your browser as an opt-out request. The site does not track you across other sites, so it does not respond differently to Do Not Track signals.

Sensitive information. The only sensitive personal information we receive is the login or key to your CRM. We use it only to provide the Sales Signal you asked for, and never to infer anything about you.

Children. Our services are for businesses and are not directed at children under 16. We do not knowingly collect their information.

Cookies. This site uses no advertising or tracking cookies, and no analytics that identify you. Fonts and scripts are served from our own servers, so opening a page sends nothing to anyone else.

Changes. This is version PN-US-2. When this notice changes, we update the version and the date at the top. If a change affects how we use information you have already given us, we tell you before it applies.