AXIOMATIC

Privacy statement

We do not sell personal data, we do not use it for advertising, and we train no model on the data of organisations. No one in an organisation reads its staff's conversations with Inora. Below is what we process on our website, when you contact us and in Inora, why, where and for how long, who else handles it, and what rights you have.

Updated on 9 November 2026

Who we are

Axiomatic B.V. is a software company in Delft, the Netherlands, registered with the Dutch Chamber of Commerce under number 97816825. We design and build Inora, implement it ourselves and run it.

Our data protection officer is an external DPO, reachable at fg@axiomatic.digital and notified to the Dutch Data Protection Authority. For other questions about this statement, write to privacy@axiomatic.digital.

Two roles: for ourselves and for care organisations

This statement distinguishes two roles under the GDPR. The controller decides why and how data is processed. The processor processes data on the controller's behalf and on its instructions.

For our own work, we are the controller. That covers the website, email you send us, our relationship with customers and prospective customers, and job applications. The sections from "The website" to "At a glance" describe this.

For Inora, the care organisation is the controller and we are the processor. The organisation determines the purposes for which it uses Inora, which documents go into it, which staff use it and how long conversations are kept. We process that data only on the organisation's instructions, under a data processing agreement that meets Article 28 of the GDPR. The section "Inora: what we process for care organisations" describes this. That explanation does not replace the care organisation's privacy notice or the data processing agreement.

If you work at a care organisation that uses Inora, or receive care from one, that organisation decides what happens with your data. Ask the organisation first. If you contact us, we forward your request to the organisation and help it answer.

The website

We want to know how our website is read, and by which organisations. For that we use PostHog, a web analytics service. PostHog's script is part of our own website's files and sends through our own domain to PostHog's EU cloud.

What PostHog receives. Which pages you view, how far you read and when you leave; where you click, what you copy and which documents you download; a recording of your visit, with what you see, where you move and click and what you type into a form, also before you press Send; the requests the page makes, with their contents, their headers and their timing; messages and errors in the browser's console; how fast the page loads (Web Vitals); the page, search engine or campaign you came from; your IP address, which we do not shorten, and your browser. An identifier in a cookie and in your browser's local storage links your visits together.

When we know who you are. If you send a form, PostHog links your visits, the earlier ones too, to the email address, name, role and organisation you entered. If you open a link we sent you personally, it carries a code only we can connect to your name; your visits then join your details as well. Visitors with a work email address at the same organisation are brought together under that organisation in PostHog.

Which organisation a visit comes from. For visits we cannot link to a name, we ask IPinfo afterwards which organisation the IP address belongs to, and add that organisation to the visit. This happens on our servers, not in your browser.

The chat. As soon as you scroll, click or press a key on a page, Intercom's chat loads, from Intercom's domains. From then on Intercom receives your IP address, your browser, the page you are viewing and what you write in the chat. If you have sent a form, the chat also receives your name and email address, so we can answer you there. In the chat Ax answers first: an AI assistant (Fin, by Intercom) that answers from the public pages of this website; each of Ax's answers carries the label 'AI Agent'. Our team reads along and takes over the conversation when you ask.

Why. To see how the website is used and where it fails; to know which organisations are looking into Inora, so we can help them at the right moment with the right information; and to answer you in the chat. Legal basis: our legitimate interest (Article 6(1)(f) GDPR). We do not use this data for advertising, never sell it, and it never goes into Inora.

Who processes it. PostHog, Inc. (United States), in its EU cloud: the data is stored in Germany, on Amazon Web Services. Intercom R&D Unlimited Company (Ireland): the chat is stored in the United States, with Intercom, Inc. and Amazon Web Services. IPinfo, Inc. (United States), which receives only the IP address. All three process the data as our processors and are listed under Sub-processors. PostHog and Intercom, Inc. take part in the EU-U.S. Data Privacy Framework, and their data processing agreements add the EU standard contractual clauses (posthog.com/dpa, posthog.com/subprocessors, intercom.com/legal/data-processing-agreement).

How long. We keep recordings for 30 days. PostHog keeps events and the visitor profile, with the name, email address and organisation linked to it, for seven years, the term of our plan (posthog.com/docs/data/events-retention). We keep chat conversations at Intercom until two years after the last contact, as we do our email. On request we delete everything sooner.

Objecting. Write to privacy@axiomatic.digital with the date and time of your visit, or the email address you entered. We then delete your recordings, events and profile at PostHog, and your conversations at Intercom (Article 21 GDPR). You can also stop it yourself: switch JavaScript off for axiomatic.digital, and nothing goes to PostHog or Intercom; every page still reads without it. If you block only cookies and local storage, PostHog no longer links your visits together, but it still records each visit.

Fonts, images, styles and PostHog's script come from our own domain. Only the chat loads from Intercom's domains, and only after you scroll, click or type.

The site is hosted on Amazon Web Services: its files are stored in the Europe (Ireland) Region and Amazon CloudFront delivers them. To deliver a page and protect the site against attacks, CloudFront processes the technical data every web request carries: your IP address, the page requested, the time, and your browser's identification. We switch on no access logs and keep none ourselves. CloudFront may serve a page from a location outside the European Union; see "Where data is stored".

Legal basis for delivering and securing it: our legitimate interest (Article 6(1)(f) GDPR).

Email and contact

When you email us, we keep your message, your name, your email address and whatever else you include, so that we can answer and have the history at hand if you write again. Our email runs on Google Workspace.

We keep correspondence for two years after the last contact, unless it becomes part of a customer relationship or we must keep it longer by law.

Legal basis: our legitimate interest in answering you (Article 6(1)(f) GDPR). Article 6(1)(b) applies to steps you request before entering into a contract to which you personally will be a party. A contract with your employer is not a contract with you.

You choose whether to email us and what to include. Without enough contact information and detail, we may not be able to answer. Do not include client data.

If you use the contact form

What we receive. Through “Talk to our team” on every page and on /en/contact we receive your email address, first name, last name, role, organisation, size band in FTE, field of care and your answer to “Which work takes your team the most time now?”. We also receive the language, the time, the page you opened the form on and what that page passed on: field, route and number of care workers. We do not ask for a phone number.

What goes to PostHog and Intercom. The recording of your visit contains the form as you fill it in, and the request that sends it, with its contents. After you send it, PostHog links your visits to your email address, name, role and organisation, and brings you together with others from your organisation (see ‘The website’). Intercom’s chat receives your name and email address.

Why. We process this data to answer you, on the basis of our legitimate interest (Article 6(1)(f) GDPR). Where it concerns steps towards an agreement, Article 6(1)(b) GDPR applies.

How long. Axiomatic keeps the data for twelve months; then the system deletes it by itself. A copy may remain in the backup for 35 days. The email itself we keep as correspondence; see “Email and contact”.

Who receives it. Our team receives your message by email. Storage and sending run on Amazon Web Services in the Europe (Ireland) region; the email arrives at Google Workspace. Both are on Sub-processors.

Deletion or access. Write to privacy@axiomatic.digital.

If you take the AI scan

The AI scan at /en/scan works out your result in your own browser. Your answers only reach us as a request when you press Send. PostHog does record your visit, as on every page, including what you click and type in the scan before you send it (see ‘The website’). The email field is in that recording too, and so is the request the page makes when you send, with your answers and your email address. The scan itself sets no cookie of its own. The scan’s first question is also on Start with Inora: if you choose an answer there, it travels in the page address to the scan, and PostHog sees that address too.

What we receive when you press Send. Your answers to the ten questions, the result that follows from them, the language of the page and the time, and whatever you chose on the page you came to the scan from. If you enter your email address, we receive that too. The scan’s own storage does not keep your IP address. To limit abuse, we do count how many requests come from the same address within an hour, under a salted hash of that address, kept apart from your answers. The salt changes every hour, and after that hour we no longer use the hash; the system deletes it automatically, usually within a few days, and a copy may remain in our backup for another 35 days.

What also goes to PostHog. When you send, a copy of your answers and the result goes to PostHog, with your IP address, your browser and the country you opened the page from, linked to your visit. If you enter your email address, PostHog links your visits to it (see ‘The website’). The same consent covers that copy; if you withdraw it, we also delete your profile and events at PostHog.

Why. We use your answers and, if you enter it, your email address to send you the result and get in touch with you about it, on the basis of your consent, which you give by pressing Send; you can withdraw it at any time.

How long. At Axiomatic we keep the answers and the email address for twelve months; then the system deletes them by itself, and a copy may remain in our backup for 35 days after that. The email with your answers in our mailbox we keep as correspondence (see “Email and contact”). The copy at PostHog, like the rest of your visit, stays for seven years, the term of our plan at PostHog, unless you ask us to delete it sooner; we then delete your profile and your events at PostHog.

Who receives it. At Axiomatic, only Ahsan Fazal, who answers the scan. Storage and sending run on Amazon Web Services in the Europe (Ireland) Region; the email arrives in our mailbox at Google Workspace; PostHog receives the copy above. All three are listed under Sub-processors. We do not sell your data or share it with anyone else.

Deletion or access. Write to privacy@axiomatic.digital from the address you entered, or name it. We then delete your data, at PostHog too. You ask for access or correction the same way. If you disagree with how we handle your data, you can lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

Customers and prospective customers

For each organisation we work with, we keep the names, work email addresses, phone numbers and roles of the people we deal with, the agreements we sign, and our invoices. We need this to prepare, perform and invoice the agreement. We receive contact details from you or from your organisation.

We keep contact details for as long as the relationship lasts and for two years after it ends. We keep invoices and the records behind them for seven years, because Dutch tax law requires it.

Legal basis: our legitimate interest in working with the organisation that employs you (Article 6(1)(f) GDPR), and our legal obligation to keep financial records (Article 6(1)(c) GDPR).

Axiomatic takes no card payments. Customers pay by bank transfer against an invoice.

Applying for a job

If you apply for a job at Axiomatic, we keep your application, CV, correspondence and notes from interviews. Only the people involved in the selection see them. Without the information needed for the role, we cannot assess your application.

We delete your data no later than four weeks after the procedure ends. With your consent, we keep it for up to one year after the procedure ends so we can contact you about another role. You can withdraw that consent at any time.

Legal basis: steps before entering into an employment contract (Article 6(1)(b) GDPR); for the longer period, your consent (Article 6(1)(a) GDPR).

At a glance

Data	Purpose	Legal basis	Retention
Technical request data on the website (IP address, page, time, browser)	Delivering and protecting the website	Legitimate interest	No access logs held by Axiomatic
Website visits in PostHog (pages, clicks, a recording of the visit with what you type, where you came from, IP address, browser; after a form or a personal link your name, email address, role and organisation)	Seeing how the website is used and by which organisations	Legitimate interest	Recordings 30 days; events and visitor profile seven years, sooner on request
The organisation behind an IP address (IPinfo)	Knowing which organisation a visit comes from	Legitimate interest	With the visitor profile in PostHog, seven years
The chat (Intercom)	Answering you	Legitimate interest	Two years after the last contact
The AI scan you send (answers, result, email address if given)	Sending you the result and contact about it	Consent	Twelve months at Axiomatic; the copy at PostHog seven years; sooner on request
The submitted contact form (contact and organisation details, role, size band, field of care, message)	Answering your message and steps towards an agreement	Legitimate interest; steps towards an agreement	Twelve months at Axiomatic; then up to 35 days in the backup
Email correspondence	Answering and keeping the history	Legitimate interest; steps before a contract	Two years after the last contact
Contact details of customer staff	Preparing and performing agreements	Legitimate interest	The relationship plus two years
Invoices and financial records	Invoicing and tax	Legal obligation	Seven years
Job applications	Selection	Steps before a contract; consent for longer retention	Four weeks after the procedure; one year with consent

Data	Purpose	Legal basis	Retention
Data in Inora	On behalf of the care organisation	Determined by the organisation as controller	See “Inora” and “Retention and deletion”

Inora: what we process for care organisations

Inora lets care workers ask questions in ordinary language and get answers from their organisation’s sources, with each of the organisation’s sources marked in the answer and the passage one tap away. To do that, it processes twelve kinds of data on behalf of each organisation, in the order of Annex 1 to the data processing agreement.

1. Documents. The protocols, guidelines, work agreements, procedures and quality handbook the organisation adds. They may contain names of staff, such as authors and owners.

2. Questions, answers and reports. Questions can be typed or spoken. What users ask, what Inora answers, which sources it shows, and the reports it drafts in the organisation’s format, such as SBAR or SOAP.

For the team reports (see “Staff conversations”) the language model that writes the answer sorts the conversation by topic in the same step, without names. No person reads along, and the sorting stays in the environment and is deleted with the conversation.

3. User accounts. Inora receives a user’s name, work email address, a unique identifier and group membership from the organisation’s own single sign-on. With single sign-on Inora stores no passwords.

4. Logs. Sign-ins, administrative actions, and technical data such as IP addresses and times, to keep the service secure and to investigate problems.

On request the organisation receives the logging only totalled per team of at least five people and per day; one member of staff’s sign-in times and IP addresses never. In a security incident we investigate the log ourselves and report a finding about the system, naming no care worker.

5. Support and implementation. Only the documents the organisation asks us to look at, under the period of the processing it belongs to; a conversation only as “Staff conversations” describes, a legal demand included. We make no copies outside its environment.

6. Service metrics. Question counts and response times per user, without content and without names, only to run the organisation's own environment and fix problems in it. Per user we keep them for 30 days, after that only totalled per team of at least five people. The organisation never receives them per member of staff.

7. Competence record. The competence record the inspectorate expects (Wkkgz, Wet BIG), for reserved and high-risk procedures under the organisation's training policy. Per member of staff it records only which procedure was performed, under which protocol and version, on which date and on whose instruction, which assessor signed off the practical assessment, how long the competence holds and when reassessment is due, never the content of a conversation, a score or a usage figure. The competence lapses when the care worker has not performed the procedure for a long time. It is the organisation's own record; we keep it in Inora as processor, on its instruction, as "Staff conversations" describes.

8. Test set. Questions from the organisation, and answers a member of staff or a check flagged with their question, stripped of the names of clients and staff. We keep them only on the organisation's written instruction, after the works council's consent where it has one, to test every new version of Inora before it goes live, and for nothing else: not to train models and not for another organisation. The same language model in the EU that gives the answers removes the names; no person reads a conversation for it, and no member of Axiomatic's staff reads a question or answer in the test set: testing a new version is automated. We keep them until the organisation withdraws the instruction, at the latest until the end of the agreement, and delete them within 30 days after that.

9. Answer record. For every answer Inora records what it rested on: the sources with their versions, the check it passed and the date, and a reference the member of staff sees with the answer. Who asked, the time, the ward, the question and the answer are not in it. The record stays with us, never at the organisation; it receives the record only on a written request, for an incident or a complaint, and never who asked.

10. Usage research. Axiomatic processes anonymised usage data from Inora for its own research, and is itself the controller for it.

11. Record data (register P10). Once Inora reads the record, through a connection or the user's own login, Inora reads from the client record what the task under way needs, with the rights of whoever does the work: a question, preparing a visit, a review, a rule or signal, at night too. Inora keeps no second record.

12. Record log (register P11). Once Inora reads the record, through a connection or the user's own login, Inora records per step what it did, on whose behalf, for which client and with what result, set up to NEN 7513. The function the organisation appoints sees it only on written

request, per client or in an investigation. What anyone asks is never in it.

Questions, answers and reports can contain information about clients, including information about their health. The GDPR treats health data as a special category. Inora keeps no second client file and does not ask for a citizen service number (BSN). We treat everything users type into Inora as health data, and protect it as such.

The organisation must establish a legal basis under Article 6 GDPR for each processing activity. Health data also requires an exception to the prohibition in Article 9 GDPR. Article 9(2)(h), together with Article 30(3)(a) of the Dutch GDPR Implementation Act (UAVG), may apply to necessary processing for treatment, care or the management of a care institution. It does not automatically cover every use of Inora. The organisation assesses necessity, the legal basis and professional confidentiality before allowing that processing. Article 9(3) GDPR and Article 30(4) UAVG impose confidentiality requirements. Everyone at Axiomatic has signed a confidentiality agreement for that reason.

What we do with this data: only what the data processing agreement and the organisation's instructions say. What we do not do with it:

- We do not use it for our own purposes, except the anonymous counts of the usage research, for which we are the controller ourselves.
- We do not use it to train or fine-tune models, and our model provider does not either.
- We do not sell it or share it with other customers. Disclosure to sub-processors or public authorities is limited to the cases below.
- We do not combine one organisation's data with another's. Each organisation has its own environment. Only the anonymous counts from the usage research are totalled by us over at least five organisations.
- We do not look at the content of conversations and documents, except in the cases listed under "When we access or disclose data".

The service metrics contain no document, question or answer content and no names. That does not automatically make them anonymous: a measurement without a name may still identify a person. We therefore treat them as personal data under the data processing agreement. We do not use them for our own purposes or to compare organisations.

Staff conversations

What a member of staff asks Inora, no one in the organisation reads; Axiomatic only by the rules below. For the organisation they work for, and for us, this holds:

- **No one in the organisation reads a conversation, management included.** No administrator, manager or board member can open a member of staff's questions and answers in Inora.
- **Reports cover teams of at least five people.** The monthly report shows, per team, the topics staff ask about and the topics that found no answer yet, with a count, never a question as someone typed it and never per person. Per team it goes to the team lead and the works council; the board and quality receive the sum across all teams. A team of fewer than five people gets no report of its own. Inora assesses no one and gives no one a score.
- **A question without an answer goes to the owner as a topic.** When the answer is not in the sources, whoever owns the subject receives the topic, rewritten without identifying detail and without the asker's words, with the number of times it was asked, pooled per protocol and summed across all teams, so the source can be completed. The name of whoever asked does not go with it.
- **We read a conversation only on a written request, for a stated purpose.** Axiomatic reads a conversation only on a written request from the function the organisation names, for an incident or a complaint; every access is logged and the member of staff is told. In an outage or security incident Axiomatic examines the system logs and the answer record, never a conversation. Whoever made the request gets a finding about Inora, never what the member of staff asked or read. The function is named in the data processing agreement, such as the data protection officer, and we read only what the purpose needs.

What a care worker asks Inora never reaches the organisation. Only what the care worker sends reaches it, such as a report or an incident report, and the competence record the inspectorate expects (Wkkgz, Wet BIG). That record covers reserved and high-risk procedures under the organisation's training policy, and it is the organisation's own record. It records only the procedure, the protocol with its version, the date and on whose instruction, never the content of a conversation, a score or a usage figure, and Article 5.6 of the data processing agreement binds it. The member of staff sees their own competence record in Inora at any time and can ask for a copy to take with them: that is their right of access (Article 15 GDPR), which the organisation answers and we help with. An incident report they send to the incident committee themselves reaches it as they send it. For the data protection officer it is all together on Privacy and data protection, for the works council on Works council.

Artificial intelligence

When a user asks a question, Inora searches the sources the organisation has designated for the relevant passages. A language model then writes an answer from those passages. In the answer, each of the organisation's sources is marked, and one tap shows the passage. If the answer is not in the sources, Inora says so. The markers make every answer checkable: the member of staff sees where it comes from and checks it themselves.

By default, the language model runs in Amazon Bedrock, from Amazon Web Services, through the EU inference profile, which processes data only in Regions within the European Union. To produce an answer, the service processes the question and the passages found. When documents are made searchable, an embedding model also processes document passages; their numerical representations are stored in the organisation's search index. Amazon Web Services does not use this data to train models. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker.

For the team reports the language model that writes the answer sorts the conversation by topic in the same step, in the EU. No person reads along, and the model keeps nothing.

The system picks the language model for each task, through Amazon Bedrock or through Azure OpenAI from Microsoft Ireland Operations Limited, in an EU region. Axiomatic runs Azure OpenAI with the modified abuse monitoring Microsoft approves for sensitive data: Microsoft stores no questions or answers, and no Microsoft employee reads them (Microsoft on abuse monitoring). Microsoft does not use this data to train models either.

Axiomatic does not train or fine-tune models on organisation data.

Inora supports professionals with their organisation's knowledge. It does not diagnose or decide on treatment; the professional decides. Its intended use keeps it outside the scope of the medical device rules.

We use AI tools internally to help write software. Those tools receive no data from care organisations.

When we access or disclose data

To provide Inora. We use as few sub-processors as we can. For hosting and the language model, those are Amazon Web Services and Microsoft Ireland Operations Limited (Azure OpenAI, in an EU region). Who processes what, and where, is on Sub-processors. Each sub-

processor has signed an agreement with data protection obligations no weaker than ours. We announce a new sub-processor to our customers 30 days before it starts. A customer can object.

For our own work. Amazon Web Services hosts the website and the AI scan. Google Workspace carries our email and documents; notices we send by email name the kinds of data and the number of people affected, never data from Inora. PostHog measures how the website is used and records visits, as ‘The website’ describes. These services never receive data from Inora.

On the organisation’s written request. We look at the content of a conversation only as “Staff conversations” describes: on a written request from the function the organisation names for it, for an incident or a complaint. We log every access, and the member of staff is told. We do not disclose to the organisation what the member of staff asked or read. By the same route the organisation receives the answer record of an answer, never who asked.

To handle an incident. In a security incident or a failure we examine the system logs and the answer record, and look only at what is needed to resolve it; we do not then read a member of staff’s conversation. We tell the organisation.

When the law requires it. We disclose data to a government authority only when Union or Dutch law obliges us to, for example under a court order. We then disclose no more than required. Unless the law forbids it, we tell the organisation before we disclose anything. We object to requests that do not have a valid legal basis. If the law demands a conversation, Axiomatic gives only what the demand asks, logs it, and the member of staff is told, unless the law forbids it.

If Axiomatic is acquired. We inform customers before their personal data moves to another company or becomes subject to another policy. An acquisition does not in itself provide a legal basis for using data differently.

Where data is stored

Inora, for organisations in the EU. For an organisation in the European Union, all Inora data is processed and stored in the EU. Production and backups run on Amazon Web Services in the Europe (Ireland) Region. The language model runs in the EU. Processing outside the EU first requires a written amendment to the arrangements with the organisation. Transfers outside

the European Economic Area also require a valid basis under Chapter V GDPR; the organisation's authorisation alone is not enough. This includes remote access by a recipient outside the EEA.

Amazon Web Services EMEA SARL in Luxembourg provides these services, and so does Microsoft Ireland Operations Limited in Dublin. Their parent companies, Amazon.com, Inc. and Microsoft Corporation, are American and both are listed under the EU-U.S. Data Privacy Framework. Storage in the EU does not rule out a request from a foreign government. We object to one without a valid legal basis, and tell the organisation first unless the law forbids it.

Inora, for organisations outside the EU. When an organisation outside the European Union works with Inora, its environment runs in its own country, with a supplier and in a region its data processing agreement names. Data of organisations in the EU never goes there.

The website and our email. Amazon, Google, PostHog, Intercom and IPinfo are American companies or part of one. A web request can be served from outside the EU, and email we send and receive can be stored outside the EU. What PostHog receives about your visit is stored in Germany; the chat is stored with Intercom in the United States; IPinfo receives the IP address in the United States. Amazon.com, Inc., Google LLC, PostHog, Inc. and Intercom, Inc. are listed under the EU-U.S. Data Privacy Framework; the data processing agreements of PostHog and Intercom add the EU standard contractual clauses. You can ask which safeguards apply and request a copy at privacy@axiomatic.digital.

How we secure data

Data in Inora is encrypted in transit and at rest. Each organisation has its own environment. Staff sign in through the organisation's own single sign-on. Only the engineers who build and operate Inora, named in the data processing agreement, have access to production, each with a personal account and multi-factor authentication, and every access is logged. Axiomatic's advisers have no access to organisation data. The measures are on Security.

For a breach involving data for which we are controller, we assess the duties under Articles 33 and 34 GDPR. We notify the Autoriteit Persoonsgegevens without undue delay and, where feasible, within 72 hours of becoming aware, unless a risk to people's rights and freedoms is unlikely. Where a high risk is likely, we inform affected people without undue delay, unless an exception under Article 34(3) applies. We document every personal data breach. For Inora, we notify the organisation as Security describes.

Retention and deletion

Conversations in Inora (questions, answers and drafted reports) are kept for 90 days by default and then deleted. The organisation can set a shorter or longer period. If the function the organisation names for it asks, within the retention term, for a conversation for an incident or a complaint, Axiomatic holds it until the investigation is complete, deletes it within 30 days after that, and the member of staff is told.

Documents stay in Inora as long as the organisation keeps them there. When the organisation removes a document, Inora stops using it at once. Copies in backups are deleted within 30 days.

User accounts are kept for as long as a user has access and up to 30 days afterwards.

Logs are kept for 12 months, unless the agreement ends sooner.

Service metrics are kept per user for 30 days, after that only totalled per team of at least five people.

The competence record stays in Inora for as long as the member of staff works for the organisation, plus 30 days; in those 30 days the organisation exports it to its own personnel file, where its own term applies.

The test set is kept until the organisation withdraws the instruction, at the latest until the end of the agreement, and deleted within 30 days after that.

The answer record stays with us for 2 years and is then deleted by itself; from backups within 30 days.

The sorting by topic is deleted with the conversation.

Backups: daily, encrypted, kept for 30 days, in the Europe (Ireland) Region.

When an agreement ends, the organisation chooses return or deletion. We keep the data available for return up to and including day 30, unless the organisation requests earlier deletion or confirms that return is complete. We delete the data from active systems, including logs and search indexes, no later than day 30. Backup copies are deleted no later than day 60. Only a retention requirement under Union or Dutch law can justify an exception; we then state the data, legal basis and period concerned, unless the law prohibits this. The data remains protected for as long as we hold it. On request, we confirm deletion in writing.

After deletion during the agreement, data may remain in backups for up to 30 further days. We reapply deletions after a restore. This also covers conversations, account data and associated search data.

For data we process as controller, the periods are in “At a glance”.

Your rights

You have the following rights with respect to data we process as controller, subject to the conditions in the GDPR. For data in Inora, the care organisation handles these requests; we forward yours to it within two working days and help it answer.

- **Access.** You can ask which personal data we hold about you and what we do with it.
- **Rectification.** You can ask us to correct data that is wrong or incomplete.
- **Erasure.** You can ask us to delete your data. We do so where the GDPR requires it. Exceptions include a statutory retention duty or the establishment, exercise or defence of legal claims.
- **Restriction.** You can ask us to stop using your data for a period, for example while we check whether it is correct.
- **Portability.** Where we process data you provided by automated means on the basis of your consent or a contract with you, you can receive it in a structured, commonly used and machine-readable format. Where technically feasible, you can have it transferred directly to another controller.
- **Objection.** Where we rely on our legitimate interest, you can object. We stop unless we demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed for legal claims.
- **Withdrawing consent.** Where we rely on your consent, you can withdraw it at any time. This does not affect the lawfulness of processing before withdrawal.
- **No automated decisions.** We make no decisions about you by automated means alone.

Email privacy@axiomatic.digital. Requests are normally free of charge. We respond without undue delay, no later than one month after receipt. Where the complexity or number of requests requires it, that period may be extended by up to two further months. We tell you within the first month, with the reason. If we refuse your request, we explain why and how you can complain or seek a judicial remedy.

Where we have reasonable doubts about your identity, we ask only for the additional information needed to confirm it. Someone acting on your behalf must demonstrate their authority; signed authorisation is one way to do so.

Complaints

You can complain directly to the Dutch Data Protection Authority, the Autoriteit Persoonsgegevens, at autoriteitpersoonsgegevens.nl or by post: Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag. You do not have to contact us first. You can also complain to the competent authority in the EU country where you usually live or work, or where the suspected infringement occurred.

Changes and questions

We change this statement when the law, our services or our sub-processors change. The date at the top shows the latest version. We email our customers' contacts 30 days before a material change takes effect.

Questions about this statement, your data or your rights: privacy@axiomatic.digital.