AXIOMATIC

Supplier file

Every Axiomatic B.V. document on Inora, with who it is for and when it arrives.

7 November 2026

Contents

IT and security pack	page 6
Security overview	page 14
Control matrix	page 24
Sub-processors	page 37
Privacy pack	page 41
Pack for the works council	page 51
Information letter and model consent request	page 63
Quality and clinical pack	page 73
Privacy statement	page 87
Responsible disclosure	page 104

All documents

Before the first question

Document	For	Where
Sub-processors Who else processes data, and where.	Data protection officer, IT	page 37

Document	For	Where
Control matrix Every control of NEN 7510 and ISO 27001, and how we built it. Updated every quarter and checked once a year against what runs in production. The basis for your statement of applicability.	Board of directors, IT	page 24
IT and security pack What day one costs your team, where the data is, who can reach it, and every measure.	IT	page 6
Privacy pack with the DPIA pre-filled The DPIA pre-filled: the roles, and each processing with its purpose, place and period.	Data protection officer	page 41
Works council pack What reaches the organisation and what never does, the team report, each rule's clause.	Works council	page 51
Quality and clinical pack Your protocols set every answer, every document has an owner, and with any failure the system is what gets examined.	Nursing advisory council, Quality and safety	page 73
Security overview (full) Every security measure, and the connection to your identity provider.	Board of directors, IT	page 14
Security Inora and your data are secured, with fixed measures for protection and recovery.	IT	Online at axiomatic.digital
Privacy statement What we process, why, where and for how long.	Data protection officer, Works council	page 87
Instructions for use What Inora does and never does, how you deploy it, and who oversees its use.	Nursing advisory council, Quality and safety	On request, no conditions
Continuity Your knowledge if you stop, if we stop, or if Axiomatic changes hands.	Board of directors, Supervisory board, Data protection officer, Procurement	Online at axiomatic.digital
Responsible disclosure How to report a vulnerability in Inora or on this site, and what we do next.	IT	page 104

Document	For	Where
Licence list For every source that is not your organisation's own: the basis on which Inora uses it.	Quality and safety	On request, no conditions
Outcome of the intake of your handbook What is filed twice, contradicts itself or has expired, document by document, with the reason.	Quality and safety	Confidential: for its reader only, with your organisation's data
Information letter and model consent request What Inora processes and keeps, who sees what, and that no report names an employee.	Works council	page 63
One page for the nursing advisory council What Inora does and never does. A new guideline counts only after the council or your own route for documents: owner, author, two content experts, quality adviser.	Nursing advisory council	On request, no conditions
Brief for the client council What changes for clients when their care team works with Inora.	Client council	On request, no conditions
The entry for your AI register Ready to file: the provider, the intended use, which data where, and who answers for it.	Board of directors, Quality and safety	On request, no conditions
One page for the supervisory board What Inora does and where it stops, who is provider and who deployer, and which figures go in each quarter.	Supervisory board	On request, no conditions

With the agreement

Document	For	Where
The intended use, word for word What Inora does and never does, to quote as it stands. It keeps Inora outside the MDR.	Board of directors, Quality and safety	Online at axiomatic.digital

Every month

Document	For	Where
Monthly report per team Per team to the team lead and the works council, teams of five or more, never per person.	Works council	Confidential: for its reader only, with your organisation's data
Monthly report across all teams Summed across all teams, for the board and quality; no report per team, no name.	Board of directors, Quality and safety	Confidential: for its reader only, with your organisation's data

Every quarter

Document	For	Where
Figures across all teams for the quarterly report For the supervisory board each quarter, alongside the audits and incident analyses.	Board of directors, Supervisory board	Confidential: for its reader only, with your organisation's data

With every new version

Document	For	Where
What changed, with every new version What each new version changes, with the outcome of the test: new features announced ahead, security updates reported afterwards.	IT, Quality and safety	Confidential: for its reader only, with your organisation's data

After an incident

Document	For	Where
Notice and report of a data breach Our notice within 24 hours, then our report.	Board of directors, Data protection officer	Confidential: for its reader only, with your organisation's data

On request

Document	For	Where
Briefing for your board's training For the Dutch Cybersecurity Act (Cyberbeveiligingswet): what Inora is, where it stops and how it is secured.	Board of directors	On request, no conditions

AXIOMATIC

IT and security pack

Inora, for the CISO and the IT manager

Version 1.13, 11 November 2026

1. What this pack settles

You are the CISO or IT manager of a care organisation, and a colleague wants to start with Inora. Your question: does this cost my team work? This pack answers it fully enough for you to say yes in one meeting, and it is set out for your own archive.

Inora is the organisation's knowledge system: care workers get answers from its own protocols and working agreements. Axiomatic builds Inora, implements it itself and runs it. Inora is built to NEN 7510 and ISO 27001.

In short:

- **Your team does nothing to start.** One consent in your identity provider. Nothing else. Staff sign in with single sign-on; there is nothing to install.
- **Your data never leaves the EU.** One environment of your own at Amazon Web Services in Ireland, the language model in EU Regions, or everything on your own servers.
- **Only the engineers who build Inora can reach production:** each named in the processing agreement. Personal accounts with MFA, every access logged.
- **Every control is in writing**, in the control matrix in chapter 5.
- **What the Dutch Cybersecurity Act (Cbw) asks of your board is ready**, duty by duty with its document.

2. Why you are right to ask

- **Decree on electronic data processing by care providers, article 3(2).** The care provider ensures, in accordance with NEN 7510 and NEN 7512, the safe and careful use of the care information system. Source: wetten.overheid.nl, BWBR0040238.
- **Health and Youth Care Inspectorate (IGJ).** A care provider that outsources its IT remains responsible for information security itself. Source: igj.nl, Questions about NEN 7510.
- **Dutch Cybersecurity Act (Cbw), in force since 15 August 2026.** Article 21(3)(d) names the security of the supply chain as part of the duty of care; article 24 puts the approval of the measures, and the knowledge to judge them, with the board; article 26 asks for an early warning within 24 hours. Source: wetten.overheid.nl, BWBR0052872.

An AI supplier is therefore a risk you carry. This pack shows how small Inora makes that risk, and where it is written down.

3. Day one: 0 hours of IT work, with single sign-on

Item	What your team does	Hours
Accounts	Nothing. Staff sign in through your own identity provider, with SAML 2.0 or OpenID Connect; SCIM keeps the accounts in step. With single sign-on Inora stores no passwords; you set MFA and password rules yourself. Without single sign-on: Inora accounts of your own, see 4.5.	0
Network	Nothing to do: no VPN, no firewall rule. The pilot needs no connection; connections come after it, and your IT turns them on. Then: Inora readies the report; the care worker reads and signs, and only on that approval does Inora file it in the client record; Inora acts on that person's behalf, never with more rights than they have.	0
Installation	Nothing. Inora is a service in the browser and the app. We do the updates. New features are announced a week ahead, with the outcome of the test; with your written instruction, after the works council's consent where you have one, we also test on your own teams' questions. Security updates go through without the week's notice, critical ones within 72 hours, after the same test; we report them afterwards.	0

Your administrator gives Inora consent once in your identity provider and picks the groups that get access; from then on SCIM keeps the accounts in step. With Entra ID, the most used, the consent in Entra ID gives Inora only `openid`, `profile`, `email` and `User.Read`, delegated and read-only; your groups arrive as a claim in the sign-in token. Inora reads only the groups you assign to the app, so the claim never overflows. No access to mail, files, Teams or SharePoint.

Your sources stay in your own document system; Inora works with a copy that your handbook manager supplies and keeps up to date. You then decide which groups of staff get access and who manages documents and settings.

4. Where it runs and who can reach it

4.1 Hosting and location

Component	Supplier	Location
Application, database, document storage, search index	Amazon Web Services EMEA SARL, Luxembourg	Region Europe (Ireland), eu-west-1
Backups	Amazon Web Services EMEA SARL	Region Europe (Ireland), eu-west-1; across several availability zones

Component	Supplier	Location
Language model and embedding model	Amazon Bedrock, through the EU inference profile	AWS Regions in the EU

If you choose, Inora runs on your own servers, inside your own network; your data processing agreement then names every supplier of that deployment.

4.2 The language model

The system picks the language model for each task, always in the EU: at Amazon Web Services or at Microsoft Azure in the EU region, with Microsoft's modified abuse monitoring. Both are on the sub-processor list. On your own servers the language model runs inside your network.

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 sorting stays in the environment and is deleted with the conversation.

No model trains on your data: not at Axiomatic, not at the model's supplier. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker. 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 (learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring). Every model, and every change to Inora, is tested before your staff work with it; with your written instruction also on your own questions.

4.3 One environment per organisation

Every organisation has its own environment: its own database, document storage and search index. A question asked within one organisation can reach only that organisation's documents. The separation is in the infrastructure, not only in the software.

4.4 Who can reach production

- Only the engineers who build and run Inora, each named in the processing agreement (annex 2). Axiomatic's advisers, and everyone else at Axiomatic, have no access to the production environment or to organisations' data.
- Personal accounts only, with multi-factor authentication. No shared accounts.
- Every access to an organisation's environment is logged (4.7).
- Everyone at Axiomatic has signed a confidentiality agreement, and everyone with access to production holds a certificate of conduct (VOG).
- Work laptops have full-disk encryption and automatic security updates. When someone leaves, their access ends the same day.

4.5 Signing in and sessions

Sign-in runs by default through the single sign-on of your own identity provider, with any provider: Entra ID, Okta, Google or any other over SAML or OpenID Connect. Your administrator sets it up in one step; SCIM creates and closes accounts. Disable an account there and that person can no longer sign in; an open session ends at most eight hours after it began.

With single sign-on Inora stores no passwords. Your administrator disables those accounts in Inora.

4.6 Encryption

- In transit: TLS 1.2 or higher, for all traffic to and from Inora and between its components.
- At rest: AES-256 for databases, document storage, search indexes and backups. The keys sit in AWS Key Management Service, in the EU; every use is logged.
- While a question is being answered, the question and the passages are decrypted only for as long as the answer is being made; the model does not keep them.

4.7 Backups, logs and updates

- Backups: daily, encrypted, kept 30 days, in the Europe (Ireland) region, across several availability zones; at most 24 hours of data is lost. Every quarter we restore a backup as a test.
- A restore from back-up takes at most 8 hours.
- Security updates for critical vulnerabilities within 72 hours, others within 30 days.

Without a connection, Inora reads the record in a microVM of its own per user, with that person's login and rights: the care worker logs in personally, Inora stores no passwords and holds the session only while the task runs; scheduled work runs on a session its named owner approved beforehand. Only in the systems the organisation names.

Inora records sign-ins, administrative actions and every access by Axiomatic staff, for 12 months. Once Inora reads the record, through a connection or the user's own login, Inora also keeps a record log, set up to NEN 7513: per step what Inora did and on whose behalf, open to the function the organisation appoints. On request an organisation receives its environment's security logging, totalled per team of at least five people and per day, and every access by Axiomatic; a day with fewer than five sign-ins shows as '<5'. The sign-in times and IP addresses of one member of staff never go to the organisation. In a security incident Axiomatic investigates the log itself and reports a finding about the system, naming no care worker.

4.8 Availability

Built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night. Report an outage to support@axiomatic.digital, day and night. During an outage your organisation's contact gets notices by email until it is resolved.

4.9 What never leaves the EU

Your data, the backups and the logs. For an organisation in the EU, Inora runs in the EU and the language model processes data only within the EU.

5. Every control, and how it is met

The control matrix: every control of ISO 27001 and the controls NEN 7510 adds for care, each with how we built it and its status. The matrix is the basis for your statement of applicability.

Every control, with how it is built, is in the Control matrix in this file.

6. Layer by layer: who checked it

6.1 Inora

Standard or test	What it covers	By
Built to NEN 7510 and ISO 27001	Every control and how it is met, in chapter 5	Axiomatic
Built for 99.9% availability	Target: 95% of outages resolved within 4 hours; a response within an hour, day and night. Outage notices by email to your contact.	Axiomatic
Penetration test, every year	The application and the infrastructure, against the OWASP Top 10 and the separation between organisations; the summary on request	An independent specialist
Continuous scanning	Code, dependencies, containers and cloud configuration, on every change and every day	Axiomatic

You can always report a vulnerability: security@axiomatic.digital, with ‘Security’ in the subject line. We confirm receipt within three working days.

6.2 The AWS and Microsoft services underneath

The certificates Amazon Web Services and Microsoft publish for the services Inora runs on, as AWS names them on its own pages on 2 November 2026, and Microsoft for Azure on its own. They are about AWS’s and Microsoft’s services, not about Axiomatic or Inora; Axiomatic does not carry them by association.

Service	Standard	What it covers	By	Source
Hosting, Europe (Ireland)	ISO/IEC 27001:2022	Information security	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Hosting	ISO/IEC 27017:2015	Security controls for cloud services	EY CertifyPoint	aws.amazon.com/compliance/iso-27017-faqs

Service	Standard	What it covers	By	Source
Hosting	ISO/IEC 27018:2019	Personal data in the cloud	EY CertifyPoint	aws.amazon.com/compliance/iso-27018-faqs
Hosting	ISO/IEC 27701:2019	Privacy information management	EY CertifyPoint	aws.amazon.com/compliance/iso-27701-faqs
Hosting	BSI C5	German cloud standard; Ireland Region in scope		aws.amazon.com/compliance/bsi-c5
Hosting	SOC 1, 2 and 3	The auditor's reports, in AWS Artifact		aws.amazon.com/compliance/services-in-scope/SOC
Amazon Bedrock	ISO/IEC 27001, 27017, 27018, 27701	Bedrock in scope, Bedrock Marketplace not	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Amazon Bedrock	ISO/IEC 42001:2023	Management of AI systems	Schellman	aws.amazon.com/compliance/iso-42001-faqs
Amazon Bedrock	BSI C5	Bedrock in scope		aws.amazon.com/compliance/services-in-scope/C5
Amazon Bedrock	SOC 1, 2 and 3	Bedrock in scope		aws.amazon.com/compliance/services-in-scope/SOC
Microsoft Azure (Azure OpenAI)	ISO/IEC 27001, 27017 and 27018	Information security, cloud services and personal data in the cloud; which Azure services are in scope is on the Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001
Microsoft Azure (Azure OpenAI)	SOC 2 Type 2	The auditor's report on Azure, every six months, available on the Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

The physical security of the data centres lies with Amazon Web Services. AWS's parent company is American; what that means is in our privacy statement.

7. The Dutch Cybersecurity Act, duty by duty

Your board's duty	Article	What we do	What you file
Duty of care	21(3)(d): the supply chain	Every control is described, with how it is met. The data processing agreement binds us to them, and we cooperate with your audit.	Security overview version 1.4 and control matrix version 1.3, of 9 November 2026; data processing agreement,
Duty to report	26: early warning within 24 hours	A personal-data breach in your environment, or a suspected one, we report no later than 24 hours after becoming aware of it, with what you need for your own notification. The report follows within ten working days.	Notice and report of a data breach; Security
Board training	24(2) to (5)	A briefing for your board: what Inora is, where it stops and how it is secured.	Briefing for your board's training (on request)
Accountability	24(1): the board approves	One party answers for it: we build Inora, implement it and run it, and stay responsible for our sub-processors.	Terms; sub-processors, version 1.6 of 11 November 2026

8. When something goes wrong

- We report a data breach, or a suspected one, without undue delay and at the latest 24 hours after we become aware of it. That is a contractual maximum, not a waiting time.
- We share at once what is known: the nature, the data and people involved, the likely consequences and the measures.
- Within ten working days we send a written report: what happened, what caused it and what we changed.
- Your 72 hours with the Dutch Data Protection Authority stay yours and do not wait for our report. Your 72 hours start when we notify you; our 24 hours come before them.
- We investigate a failure without blame, with the cause in the system.

9. Suppliers, audits and the end

- We answer for what Inora does with your sources; you for what those sources say.
- We stay responsible for our suppliers. We announce a new sub-processor 30 days ahead; you can object.
- At the end you get everything back at no charge: documents in their own format, the rest machine-readable. Everything is gone from active systems by day 30 and from backups by day 60, confirmed in writing.
- We cooperate with audits by your organisation or your auditor, on every obligation in the data processing agreement.

10. What you receive in the file

- This IT and security pack.
- The security overview, version 1.4 of 9 November 2026, with every control.
- The control matrix, version 1.3 of 9 November 2026, the basis for your statement of applicability.
- The list of sub-processors, version 1.6 of 11 November 2026.
- The terms.
- On request: the briefing for your board's training.

11. Contact

Axiomatic B.V., Delft. security@axiomatic.digital.

12. Six rules that move with the server

Whether Inora runs with us or on your servers, this still holds.

- **No model learns from your data.**
- **Every answer with its source and version.** In every answer, each of your organisation's sources is marked; one tap shows the title and the version it comes from. If the answer is not in your sources, Inora says so, and where it looked.
- **Every step recorded.** For every answer Inora records every step: which sources it read, in which version, and which check the answer passed. On your written request, Axiomatic uses that record to trace a wrong answer to its cause in the system, never to a person.
- **Built to NEN 7510 and ISO 27001.**
- **A new sub-processor, thirty days before it starts.**
- **Leave, and your knowledge comes back free.**

AXIOMATIC

Security overview

Axiomatic B.V. and Inora

Version 1.4, 9 November 2026

1. Introduction

Axiomatic B.V. designs, builds, implements and operates Inora. Care workers ask Inora questions in ordinary language and get answers from the sources their organisation has designated; one tap on a marker shows the organisation's source a sentence rests on. The organisation's own documents are internal, and the questions can concern clients. This overview describes how we protect that data: who can reach it, where it is, how it is separated, encrypted, backed up and monitored, and how we recover.

This document is meant for the privacy officer, information security officer and IT staff of a care organisation that is assessing Inora. It is part of the security measures referred to in Annex 2 of our data processing agreement. The proposed periods and measures become commitments only after confirmation and signature of the data processing agreement.

2. Organisation and people

2.1 The team

The people who build, implement and operate Inora:

- Engineering builds and operates Inora. The director is responsible for security and privacy at Axiomatic.
- Implementation and partnerships work with care organisations during implementation, without access to organisation data or to production.
- The advisors have no access to organisation data or to production.

Only named engineers have access to the production environment, listed in the processing agreement. We do not use contractors with access to production or to organisation data.

2.2 Confidentiality and screening

Everyone at Axiomatic has signed a confidentiality agreement that continues after they leave. This agreement is also what the Dutch GDPR Implementation Act requires of people who process health data without a professional duty of secrecy of their own (Article 30(4) UAVG). Everyone with access to production holds a certificate of conduct (VOG).

Everyone reads and signs our security rules when they start, and again each year.

2.3 Devices

We work on laptops with full-disk encryption, automatic security updates, a firewall and a screen lock after a few minutes. Organisation data is never stored on laptops. A lost or stolen laptop is reported the same day, and its access is revoked.

2.4 Accounts and access

- Personal accounts only. No shared accounts, no shared passwords.
- Multi-factor authentication on every account that gives access to code, infrastructure, email or documents. Administrative access to production uses a hardware security key.
- Access to production is limited to the named engineers, and to what they need.
- Every access by Axiomatic staff to an organisation's environment is logged. We review access rights every quarter.
- When someone leaves, their access ends the same day.

3. Architecture

3.1 One environment per organisation

Each organisation has its own environment in Inora: its own database, its own document storage and its own search index. There is no shared database in which organisations are separated only by a column. A question asked in one organisation can only reach that organisation's documents.

3.2 Sign-in

Inora connects to the organisation's own single sign-on, usually Microsoft Entra ID, through OpenID Connect or SAML 2.0. With single sign-on Inora stores no passwords; multi-factor authentication and password rules are set by the organisation in its own identity provider. When the organisation disables an account there, that person can no longer sign in to Inora. An existing session may remain active until revoked or expired. A session ends no later than eight hours after it starts.

The consent in Entra ID gives Inora only openid, profile, email and User.Read, delegated and read-only; the organisation's groups arrive as a claim in the sign-in token. No access to mail, files, Teams or SharePoint. Inora reads only the groups the organisation assigns to the app, so the claim never overflows. The organisation's administrator disables those accounts in Inora.

Inora has two roles. Administrators manage documents, settings and the report register. Users ask questions and draft reports. The organisation decides which groups of staff get which role.

3.3 How a question is answered

1. A user asks a question in Inora.
2. Inora searches the organisation's own index for the passages that concern the question.
3. The question and those passages go to the language model, within the European Union.
4. The model writes an answer from the passages. Inora shows the answer with a marker after each sentence that rests on one of the organisation's sources; one tap shows the document and the passage. If no passage answers the question, Inora says so, and where it looked.
5. The question, the answer and the sources are stored in the user's conversation history in the organisation's environment, for the retention period the organisation has set.

For reports, the headings come from a register the organisation maintains. The model writes only the content beneath them.

The organisation's sources stay in its own document system; Inora works with a copy that its handbook manager supplies and keeps up to date. There is no connection to that document system.

The client record stays in the organisation's own EHR. Inora reads it with the care worker's own login and rights, in a microVM of its own per user, so the pilot needs no connection. Connections come after the pilot, and the organisation's IT turns them on.

Building the search index also sends document passages to the embedding model in the EU. Answering sends the question and retrieved passages to the language model, which in the same step sorts the conversation by topic for the team reports (section 6).

4. Hosting and location

Component	Provider	Location
Application, database, document storage, search index	Amazon Web Services (Amazon Web Services EMEA SARL)	Europe (Ireland) Region, eu-west-1
Backups	Amazon Web Services	Europe (Ireland) Region, eu-west-1
Language model	Amazon Bedrock, EU inference profile	Amazon Web Services Regions in the EU
Language models through Azure OpenAI; the system picks the model	Microsoft Ireland Operations Limited (Azure OpenAI)	An Azure region in the EU
Website axiomatic.digital (no organisation data)	Amazon S3 and Amazon CloudFront	Files in the Europe (Ireland) Region; delivered through CloudFront's global network

All Inora data is processed and stored in the European Union. Processing outside the EU first requires a written amendment to the arrangements with the organisation. Transfers outside the EEA also require a valid basis under Chapter V GDPR; the organisation's authorisation alone is insufficient. Remote access and support are included in this assessment. Article 3.5 of the data processing agreement sets this out.

The physical security of the data centres is the responsibility of Amazon Web Services. AWS publishes its own certifications and audit reports. Those cover AWS's services, not Axiomatic.

The parent companies, Amazon.com, Inc. and Microsoft Corporation, are American; both take part in the EU-US Data Privacy Framework. Storage in the EU does not rule out a request from a foreign government; section 13 describes what we then do.

5. Encryption

- **In transit.** All traffic to and from Inora, and between its components, uses TLS 1.2 or higher. Older protocols are refused.
- **At rest.** Databases, document storage, search indexes and backups are encrypted with AES-256.
- **Keys.** The encryption keys sit in AWS Key Management Service, in the EU, with access restricted and every use logged.
- **Secrets.** Passwords for services, API keys and certificates are kept in a key vault, never in source code.

The limit. While a question is answered, the question and the passages are decrypted only for as long as the answer is being made; the model does not keep them. This happens on our servers and at the language model. Encryption in transit and at rest does not prevent that processing of readable text. This is not end-to-end encryption in which only the user can read the text. Staff with production access could, in principle, see content at that moment; section 2 describes who they are and how their access is logged.

6. Artificial intelligence

- **Model.** Inora uses language models in Amazon Bedrock, through the EU inference profile. Prompts and answers are processed only in Regions within the EU. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker.
- **Azure OpenAI.** The system picks the language model for each task; through Azure OpenAI it runs in an EU region. Axiomatic runs it with the modified abuse monitoring Microsoft approves for sensitive data: Microsoft stores no questions or answers, and no Microsoft employee reads them (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).
- **Team reports.** 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 sorting stays in the environment and is deleted with the conversation.
- **Training and storage.** Neither Axiomatic nor the model provider uses organisation data to train or fine-tune models.
- **Search index.** To make documents searchable, Inora converts passages into numerical representations with an embedding model in the same EU deployment. These are stored in the organisation's own index and deleted with the documents.

- **Source on one tap.** Each sentence that rests on one of the organisation's sources carries a marker; one tap shows the document and the passage. A language model can be wrong; the source lets the care worker check it.
- **Boundary.** Inora supports professionals with their organisation's knowledge. It does not diagnose, decide on treatment or assess photos of skin or wounds; in triage the nurse triages, and Inora puts the organisation's protocol beside them and flags what is missing. The professional decides. Its intended use keeps Inora outside the scope of the medical device rules.

7. Logging and monitoring

Inora records sign-ins, administrative actions and every access by Axiomatic staff, for 12 months. On request an organisation receives its environment's security logging, totalled per team of at least five people and per day, and every access by Axiomatic; a day with fewer than five sign-ins shows as '<5'. The sign-in times and IP addresses of one member of staff never go to the organisation. In a security incident Axiomatic investigates the log itself and reports a finding about the system, naming no care worker.

- Inora also records changes to documents and settings.
- We receive alerts for repeated failed sign-ins, unusual traffic, errors and unavailability.
- The logs stay in the EU and cannot be changed by the application.

8. Backups and recovery

- We back up every organisation's environment daily; at most 24 hours of data is lost. A restore from back-up takes at most 8 hours.
- Backups: daily, encrypted, kept for 30 days, in the Europe (Ireland) Region, across several availability zones.
- Every quarter we restore a backup to a separate environment to check that it is complete.
- Built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night. The organisation reports an outage to support@axiomatic.digital, day and night. During an outage the organisation's contact gets notices by email until it is resolved.

- Each of the named engineers can restore the service alone. The recovery procedure is written down.

9. Development and change

- Every change to Inora is reviewed by a second engineer before it reaches production.
- Development and testing use a separate environment with no organisation data.
- We monitor the libraries Inora depends on for known vulnerabilities. Security updates for critical vulnerabilities are applied within 72 hours, other security updates within 30 days.
- We follow the OWASP Top 10 as the checklist for web application risks.

10. Testing

- **Penetration test.** An independent specialist tests Inora every year, the application and the infrastructure, against the OWASP Top 10 and the separation between organisations. We fix critical findings within 72 hours, others within 30 days. The summary of the latest test is available on request.
- **Continuous scanning.** Code, dependencies, containers and cloud configuration are scanned automatically on every change and every day.
- **Security researchers.** Anyone can report a vulnerability to us, under the policy below.

To report a vulnerability, email security@axiomatic.digital with “Security” in the subject line. We confirm receipt within three working days. We ask researchers not to access or change others’ data, not to disrupt the service and to give us 90 days before publication. We take no legal action against research done in good faith within these rules.

11. Incident management

We follow a written incident procedure:

1. **Detect.** Alerts, reports from users, organisations or researchers.
2. **Contain.** Stop the cause and limit the damage.
3. **Assess.** Establish which organisations, data and people are involved.

4. **Notify.** We notify a personal data breach or suspected breach without undue delay, no later than 24 hours after becoming aware. This is a contractual maximum, not a waiting period. A breach can also involve loss of availability, destruction or unauthorised disclosure. We share what is known about its nature, affected data and people, likely consequences and measures. Notices name the kinds of data and the number of people affected, never data from Inora. Further information follows as it becomes available.
5. **Support.** The care organisation is the controller. It must notify the Dutch Data Protection Authority, the Autoriteit Persoonsgegevens, without undue delay and, where feasible, within 72 hours of becoming aware of a personal data breach, unless a risk to people's rights and freedoms is unlikely. Where a high risk is likely, it informs affected people without undue delay, unless an exception under Article 34(3) GDPR applies. It documents every breach, even where notification is not required. We assist it. The 72-hour period does not wait for our final report. A late notification must explain the delay.
6. **Report.** We send a written report within ten working days of becoming aware. If the investigation is ongoing, we say so and supplement the report. This does not postpone earlier notifications.
7. **Learn.** We change the system or the procedure to prevent recurrence.

12. Retention and deletion

Data	Retention
Conversations (questions, answers, drafted reports, the topic sorting)	90 days, or the period the organisation sets; a conversation the function in annex 3 to the data processing agreement asked for, until the investigation is complete (art. 5.5)
Documents	As long as the organisation keeps them in Inora; removed from backups within 30 days of removal
User accounts	While the user has access and up to 30 days afterwards
Logs	12 months, unless the agreement ends sooner
Service metrics (numbers of questions and response times per user)	Per user 30 days; after that only totalled per team of at least five people
Competence record	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

Data	Retention
Test set, only on the organisation's written instruction	Until the organisation withdraws the instruction, at the latest until the end of the agreement; then gone within 30 days
Answer record (sources, versions, model, check and date per answer, and a reference the member of staff sees with the answer)	2 years, at Axiomatic; then out of backups within 30 days
Backups	30 days
All data after the agreement ends	Return or deletion at the organisation's choice; available for return up to and including day 30 unless return is completed or earlier deletion requested; active systems, including logs and search indexes, cleared by day 30; backups cleared by day 60

Only a retention requirement under Union or Dutch law can justify an exception to deletion. 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. After deletion during the agreement, copies may remain in backups for up to 30 further days. We reapply deletions after a restore. On request, we confirm deletion in writing.

13. Government requests

We disclose organisation data to a government authority only when Union or Dutch law obliges us to, for example under a court order, and then no more than required. Unless the law forbids it, we tell the organisation first. 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.

14. Assurance

For the organisation's assessment:

- this security overview;
- the data processing agreement, covering subjects from the Brancheorganisaties Zorg model but using its own provisions;

- the list of sub-processors;
- the control matrix in section 15: every control of ISO 27001 and NEN 7510 and how we built it, the basis for your statement of applicability;
- a description of the processing, for the organisation's data protection impact assessment (DPIA).

We cooperate with audits and inspections by the organisation or its mandated auditor covering all obligations under the data processing agreement. Routine audits normally take place once a year. Additional audits remain possible where needed under Article 28 GDPR, including after an incident, indications of non-compliance, a material change or a supervisory authority request. The organisation bears the cost of its own auditor, unless the audit reveals a material failure on our part.

15. Control matrix

Built to NEN 7510 and ISO 27001: every control of Annex A of ISO/IEC 27001:2022 and the controls NEN 7510 adds for healthcare, with how Axiomatic built it for Inora and the status of each row.

Every control, with how it is built, is in the Control matrix in this file.

16. Contact

Axiomatic B.V., Delft. security@axiomatic.digital.

AXIOMATIC

Control matrix

Inora, built to NEN 7510 and ISO 27001

Version 1.3, 9 November 2026

Every control of Annex A of ISO/IEC 27001:2022, as NEN 7510 takes it over, and the eight controls NEN 7510 adds for healthcare, with how Axiomatic built it for Inora. “With AWS” means the cloud provider carries out the control, with its own audit reports as the evidence. This document is the basis for your statement of applicability in your own assessment of Inora as a supplier.

Physical controls in the data centres lie with the cloud provider, Amazon Web Services EMEA SARL, in the Europe (Ireland) Region. Who else processes data is at axiomatic.digital/en/trust/sub-processors.

Organisational (37)

No.	Control	How we built it	Status
5.1	Policies for information security	The security policy and the security overview set out how Inora is secured, and both are public. Everyone at Axiomatic reads and signs the security rules at the start and every year after. The director approves the policy and reviews it every year and after every serious security incident.	▪ In place
5.2	Information security roles and responsibilities	The director is responsible for security and privacy at Axiomatic. The security overview names who can reach production and who cannot.	▪ In place
5.3	Segregation of duties	No change reaches production without review by a second engineer. Whoever guides organi-sations through implementation has no access to production or to their data.	▪ In place

No.	Control	How we built it	Status
5.4	Management responsibilities	Management requires everyone to sign the security rules at the start and every year, and carries the responsibility for security and privacy itself.	▪ In place
5.5	Contact with authorities	In a data breach we help the organisation notify the Autoriteit Persoonsgegevens. We answer a request from an authority only where Union or Dutch law obliges us, with no more than necessary and, unless the law forbids it, after the organisation knows.	▪ In place
5.6	Contact with special interest groups	We follow the security advisories of the NCSC and Z-CERT and the security notices of every building block Inora runs on.	▪ In place
5.7	Threat intelligence	With the advisories from 5.6 we review every month which threats bear on Inora, and record it. Known vulnerabilities in the libraries are tracked automatically.	▪ In place
5.8	Information security in project management	Every implementation and every new feature starts with its security questions answered in writing: which data, who can reach it, which supplier.	▪ In place
5.9	Inventory of information and other associated assets	A register lists every system, supplier, data store and laptop, each with an owner, checked every quarter.	▪ In place
5.10	Acceptable use of information and other associated assets	The security rules everyone signs say how information and laptops may be used. Organisation data never sits on a laptop.	▪ In place
5.11	Return of assets	When someone leaves, the laptop comes back on the last working day and is wiped. Access ends the same day.	▪ In place
5.12	Classification of information	Everything users type into Inora is classed as health data and protected as such. The organisation's documents are classed as internal.	▪ In place
5.13	Labelling of information	Every environment, store and search index carries the label of its organisation and its data class in the infrastructure.	▪ In place

No.	Control	How we built it	Status
5.14	Information transfer	All traffic to and from Inora, and between its parts, is encrypted with TLS 1.2 or higher. What we do with data, and with whom, is set down in the data processing agreement.	▪ In place
5.15	Access control	The organisation decides which groups of staff get access and who administers. Only the engineers who build Inora can reach production, each by name.	▪ In place
5.16	Identity management	Staff sign in with their own account through the organisation's identity provider, by SAML or OpenID Connect; SCIM creates and closes accounts. When the organisation disables an account there, that person can no longer sign in. There are no shared accounts.	▪ In place
5.17	Authentication information	With single sign-on Inora stores no passwords. Administrative access to production needs a physical security key, and service keys and certificates sit in a key vault, never in the source code.	▪ In place
5.18	Access rights	Every quarter we review access rights. When someone leaves, their access ends the same day.	▪ In place
5.19	Information security in supplier relationships	We work with as few sub-processors as we can: for Inora Amazon Web Services, and Microsoft (Azure OpenAI, EU). We remain responsible for what our suppliers do.	▪ In place
5.20	Addressing information security within supplier agreements	Every sub-processor has signed an agreement with obligations no weaker than those in our data processing agreement.	▪ In place
5.21	Managing information security in the ICT supply chain	Inora runs on open building blocks and its language model can be exchanged, so it depends on no single vendor. The libraries it runs on are checked for known vulnerabilities.	▪ In place
5.22	Monitoring, review and change management of supplier services	We announce a new sub-processor 30 days ahead. The organisation can object. If we find no solution together, it may end the agreement for the part that cannot be delivered without the new sub-processor, at no cost.	▪ In place

No.	Control	How we built it	Status
5.23	Information security for use of cloud services	Inora runs at Amazon Web Services EMEA SARL in the Europe (Ireland) region, its language model through Amazon Bedrock's EU inference profile or through Azure OpenAI in the EU; the system picks the model. No one trains models on this data. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker, and Azure OpenAI runs with the modified abuse monitoring Microsoft approves for sensitive data, so Microsoft stores no questions or answers and no Microsoft employee reads them.	▪ In place
5.24	Information security incident management planning and preparation	A written incident procedure in seven steps: detect, contain, assess, notify, support, report and learn.	▪ In place
5.25	Assessment and decision on information security events	Every event is assessed for the organisations, data and people it touches, and placed in one of four severity classes, critical to low, as Responsible disclosure describes them.	▪ In place
5.26	Response to information security incidents	We notify the organisation of a breach, or a suspected one, no later than 24 hours after becoming aware, with what is known. A written report follows within ten working days.	▪ In place
5.27	Learning from information security incidents	We investigate every incident without blame, with the cause sought in the system, and change the system or the procedure so it does not recur.	▪ In place
5.28	Collection of evidence	In an incident we capture a snapshot of the affected environment before anything changes, with who took it and when. The logging is immutable (5.33).	▪ In place
5.29	Information security during disruption	The restore procedure is written down, so any engineer can run it alone. After a restore we apply deletions again.	▪ In place
5.30	ICT readiness for business continuity	A backup every day, a restore test every quarter, at most 24 hours of data lost. A restore from back-up takes at most 8 hours. Built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night.	▪ In place

No.	Control	How we built it	Status
5.31	Legal, statutory, regulatory and contractual requirements	The GDPR, the Dutch UAVG and the AI Act are worked through for Inora in the published policies. The data processing agreement follows Article 28 GDPR.	▪ In place
5.32	Intellectual property rights	Protocols and handbooks stay the property of the organisation that wrote them. For sources from others, such as national guidelines, their publisher's licence applies.	▪ In place
5.33	Protection of records	Logs are kept for 12 months in the EU and cannot be changed by the application. Invoices and the records behind them are kept for seven years, as Dutch tax law requires.	▪ In place
5.34	Privacy and protection of PII	The organisation is the controller, we are the processor. No one in the organisation reads a member of staff's conversation, and no model trains on the data.	▪ In place
5.35	Independent review of information security	The organisation or its auditor audits every obligation in the data processing agreement, in principle once a year.	▪ In place
5.36	Compliance with policies, rules and standards for information security	Every year we check this matrix against what runs in production; a deviation is fixed or recorded.	▪ In place
5.37	Documented operating procedures	The incident procedure and the restore procedure are written down, so any engineer can run them alone.	▪ In place

People (8)

No.	Control	How we built it	Status
6.1	Screening	Everyone with access to production holds a Dutch certificate of conduct (VOG).	▪ In place
6.2	Terms and conditions of employment	Everyone signs a confidentiality agreement that holds after they leave, and the security rules, at the start and every year after.	▪ In place

No.	Control	How we built it	Status
6.3	Information security awareness, education and training	Twice a year the team trains on phishing and on handling care data. Everyone signs the security rules at the start and every year.	▪ In place
6.4	Disciplinary process	The security rules state what follows a breach of them, from a conversation to withdrawn access and dismissal.	▪ In place
6.5	Responsibilities after termination or change of employment	Confidentiality continues after someone leaves, and their access ends the same day.	▪ In place
6.6	Confidentiality or non-disclosure agreements	Everyone at Axiomatic has signed a confidentiality agreement, as Article 30(4) UAVG asks of anyone who processes health data without a professional duty of secrecy.	▪ In place
6.7	Remote working	Work laptops have full-disk encryption, a firewall and automatic security updates, and lock after a few minutes. Organisation data never sits on a laptop.	▪ In place
6.8	Information security event reporting	A lost or stolen laptop is reported the same day. Researchers report a vulnerability by email and hear back within three working days.	▪ In place

Physical (14)

No.	Control	How we built it	Status
7.1	Physical security perimeters	Inora runs only in Amazon Web Services data centres in the EU; their physical security lies with AWS, under its own ISO/IEC 27001 and SOC 2 reports. Axiomatic's office holds no organisation data.	▣ In place at AWS
7.2	Physical entry	Axiomatic has no server room of its own; no one from Axiomatic enters a data centre. We reach Inora only remotely, with a personal account and a physical security key (the data centres themselves: 7.1).	▪ In place
7.3	Securing offices, rooms and facilities	The rooms that hold organisation data are AWS's. No Axiomatic office holds organisation data.	▣ In place at AWS

No.	Control	How we built it	Status
7.4	Physical security monitoring	AWS monitors its data centres, as its own audit reports describe.	▣ In place at AWS
7.5	Protecting against physical and environmental threats	Fire, water, power and climate in the data centres are AWS's responsibility. Backups are kept apart from production, encrypted, in the EU.	▣ In place at AWS
7.6	Working in secure areas	Work inside the data centres' secure areas is done by AWS; Axiomatic does not work there.	▣ In place at AWS
7.7	Clear desk and clear screen	Laptops lock after a few minutes unattended. Organisation data never sits on a laptop, so it never sits on a desk either.	▪ In place
7.8	Equipment siting and protection	Inora's servers are AWS's, sited and protected by AWS.	▣ In place at AWS
7.9	Security of assets off-premises	Laptops have full-disk encryption. A lost or stolen laptop is reported the same day, and its access is withdrawn.	▪ In place
7.10	Storage media	Storage holding organisation data is AWS's, encrypted with AES-256. Laptop disks are fully encrypted.	▣ In place at AWS
7.11	Supporting utilities	Power, cooling and network in the data centres are AWS's responsibility.	▣ In place at AWS
7.12	Cabling security	Cabling in the data centres is AWS's responsibility. All of Inora's traffic is encrypted, over those cables too.	▣ In place at AWS
7.13	Equipment maintenance	AWS maintains the equipment in its data centres. Laptops install security updates automatically.	▣ In place at AWS
7.14	Secure disposal or re-use of equipment	Disks that held organisation data are AWS's, which wipes or destroys them under its own audited procedure. Laptops hold no organisation data.	▣ In place at AWS

Technological (34)

No.	Control	How we built it	Status
8.1	User endpoint devices	Work laptops: full-disk encryption, a firewall, automatic updates and a screen lock. The organisation's staff use Inora in the browser, signed in through the organisation's own identity provider.	▪ In place
8.2	Privileged access rights	Only the engineers who build Inora have administrative access to production, each with a personal account, multi-factor authentication and a physical security key. Every access is logged.	▪ In place
8.3	Information access restriction	A question in one organisation can reach only that organisation's documents. No one in the organisation reads a member of staff's conversation. Axiomatic reads a conversation only on a written request from the function the organisation names, for an incident or a complaint, or on a legal demand (art. 5.6); every access is logged and the member of staff is told, unless the law forbids it. In an outage or security incident Axiomatic examines the system logs and the answer record, never a conversation. For the team reports the language model that writes the answer sorts the conversation by topic in the same step, without names; no person reads along (art. 5.6).	▪ In place
8.4	Access to source code	The source code is reachable only through a personal account with multi-factor authentication, and every change to it is reviewed by a second engineer.	▪ In place
8.5	Secure authentication	Sign-in runs through the organisation's own identity provider, by SAML or OpenID Connect, under its own multi-factor rules; SCIM creates and closes accounts. With Entra ID the consent gives Inora only openid, profile, email and User.Read, delegated and read-only; no access to mail, files, Teams or SharePoint. Inora reads only the groups the organisation assigns to the app, so the claim never overflows. A session ends no later than eight hours after it starts.	▪ In place

No.	Control	How we built it	Status
8.6	Capacity management	Load, storage and model capacity are measured per environment, with an alert before a limit is reached.	▪ In place
8.7	Protection against malware	Every document that enters Inora is scanned for malware before it reaches the search index. Laptops run the operating system's malware protection.	▪ In place
8.8	Management of technical vulnerabilities	Inora's libraries are checked automatically for known vulnerabilities. Critical security updates are applied within 72 hours, others within 30 days.	▪ In place
8.9	Configuration management	The infrastructure is defined as code and reviewed like software, by the same second engineer as a change to Inora.	▪ In place
8.10	Information deletion	Conversations are deleted after 90 days, or after the period the organisation sets; a conversation the function in annex 3 to the data processing agreement asked for stays until the investigation is complete (art. 5.5). After the agreement, active systems are empty by day 30 and backups by day 60, confirmed in writing.	▪ In place
8.11	Data masking	Development and testing use no organisation data. The measurements Axiomatic sees contain no names and no content of documents, questions or answers.	▪ In place
8.12	Data leakage prevention	A question can reach only its own organisation's documents. Organisation data never goes onto a laptop or into the AI tools we use to write software.	▪ In place
8.13	Information backup	A backup of every environment every day, encrypted, kept for 30 days, in the Europe (Ireland) region. Every quarter we restore one to check that it works.	▪ In place
8.14	Redundancy of information processing facilities	Inora runs across several availability zones of the Europe (Ireland) region, so the loss of one data centre does not stop it. The stored data also sits across several zones at AWS.	▪ In place

No.	Control	How we built it	Status
8.15	Logging	Inora records sign-ins, administrative actions and every access by Axiomatic staff, for 12 months. On request an organisation receives its environment's security logging, totalled per team of at least five people and per day, and every access by Axiomatic; a day with fewer than five sign-ins shows as '<5'. The sign-in times and IP addresses of one member of staff never go to the organisation. In a security incident Axiomatic investigates the log itself and reports a finding about the system, naming no care worker.	▪ In place
8.16	Monitoring activities	We are alerted to repeated failed sign-ins, unusual traffic, errors and unavailability.	▪ In place
8.17	Clock synchronization	Every server takes its time from the cloud provider's time service, so the logs of every part line up to the second.	▪ In place
8.18	Use of privileged utility programs	Administrative tools that can bypass the application reach production only through the engineers' personal accounts, with a physical security key. Every access is logged.	▪ In place
8.19	Installation of software on operational systems	Software reaches production only as a reviewed release through the deployment pipeline; no one installs anything on a running server by hand.	▪ In place
8.20	Networks security	All traffic to Inora and between its parts uses TLS 1.2 or higher; older protocols are refused.	▪ In place
8.21	Security of network services	Inora is reachable only through AWS's load balancer, behind a web application firewall that blocks known attack patterns.	▪ In place
8.22	Segregation of networks	Each organisation has its own environment, separated in the infrastructure and not only in the software. Development and testing run apart from production.	▪ In place
8.23	Web filtering	Work laptops filter web traffic at DNS level and block known malicious domains.	▪ In place

No.	Control	How we built it	Status
8.24	Use of cryptography	TLS 1.2 or higher in transit, AES-256 at rest for databases, document storage, search indexes and backups. The keys sit in AWS Key Management Service, in the EU; every use is logged. Secrets sit in a key vault.	▪ In place
8.25	Secure development life cycle	Every change is reviewed by a second engineer, with the OWASP Top 10 as checklist. If the organisation gives a written instruction for it, after the consent of its works council where it has one, every new version is tested on its test set, its own questions and flagged answers stripped of names, before its staff see that version.	▪ In place
8.26	Application security requirements	Beside the OWASP Top 10, what is particular to Inora counts as a security fault: an answer outside the organisation's sources, or one organisation reaching another. The severity classes on Responsible disclosure name them.	▪ In place
8.27	Secure system architecture and engineering principles	Each organisation has its own database, document storage and search index; no shared database with organisations told apart by a column. The language model can be exchanged, and processing stays in the EU.	▪ In place
8.28	Secure coding	The OWASP Top 10 is the checklist at every review. Secrets never sit in the source code, and libraries are checked for known vulnerabilities.	▪ In place
8.29	Security testing in development and acceptance	If the organisation gives a written instruction for it, after the consent of its works council where it has one, every new version is tested on its test set, its own questions and flagged answers stripped of names, before it goes live.	▪ In place
8.30	Outsourced development	Inora is built by Axiomatic's own engineers. No outside contractor has access to production or to organisation data.	▪ In place
8.31	Separation of development, test and production environments	Development and testing happen in a separate environment, without organisation data.	▪ In place

No.	Control	How we built it	Status
8.32	Change management	Every change is reviewed by a second engineer before it reaches production. Planned maintenance is announced in advance, and a function the organisation relies on is never removed unannounced.	▪ In place
8.33	Test information	Test data contains no organisation data; development and testing happen without it.	▪ In place
8.34	Protection of information systems during audit testing	Audits and tests on production are agreed in advance, read-only where possible and outside the busiest hours.	▪ In place

Healthcare (NEN 7510) (8)

No.	Control	How we built it	Status
5.38	Analysis and specification of information security requirements	Every feature is held in advance to the OWASP Top 10 and to the faults particular to Inora: an answer outside the sources, or one organisation reaching another.	▪ In place
5.39	Uniquely identifying subjects of care	Inora keeps no register of care recipients, so it has no duplicates; unique identification and merging happen in the organisation's ECD. Inora asks for no citizen service number.	▪ In place
5.40	Validation of displayed or printed data	Inora keeps no register of care recipients. A report about a client goes, on the care worker's approval, into the record of the client they have open in the ECD, where the organisation identifies the client. Every sentence that rests on a source of the organisation carries a marker that shows the document and the passage.	▪ In place
5.41	Publicly available health information	Public sources the organisation designates, such as national guidelines, are read as published, under their publisher's licence, and every answer shows the source it rests on.	▪ In place

No.	Control	How we built it	Status
5.42	Communication in emergencies	The organisation reports an outage that makes Inora unusable to support@axiomatic.digital, day and night; a response within an hour. In a breach its contact hears no later than 24 hours after we become aware. We test the channel and a second contact every year with the organisation's contact.	▪ In place
5.43	Reporting incidents externally	We notify the organisation of a breach no later than 24 hours after becoming aware and help it notify the Autoriteit Persoonsgegevens, which it must do within 72 hours where feasible.	▪ In place
6.9	Management training	Management takes training every year in the duties the Cyberbeveiligingswet and NEN 7510 place on it.	▪ In place
8.35	Zero trust principles	No access rests on a network location: every user signs in through the organisation's own identity provider, every administrative access takes a personal account and a physical key, and every access is logged.	▪ In place

Questions about this matrix: security@axiomatic.digital.

AXIOMATIC

Sub-processors

Axiomatic B.V. and Inora

Version 1.6, 11 November 2026

A sub-processor is a company we engage that processes personal data from Inora on behalf of a care organisation. We use as few as possible. Each has signed an agreement with us containing data protection obligations no weaker than those in our data processing agreement.

Inora

All sub-processors of Inora process data in the European Union.

Sub-processor	Service	Data	Location	Outside the EEA
Amazon Web Services EMEA SARL, Luxembourg	Hosting: application, database, document storage, search index and backups (Amazon Web Services)	All Inora data	Europe (Ireland) Region, eu-west-1	No

Sub-processor	Service	Data	Location	Outside the EEA
Amazon Web Services EMEA SARL, Luxembourg	Language and embedding models (Amazon Bedrock, EU inference profile)	Questions, typed or spoken, and passages found while the answer is written, with the model sorting the topic for the team reports in the same step; on a written instruction, the contents of the test set, to remove the names; document passages when the search index is built; not used for training; Bedrock does not store the question or the passages and does not pass them to the model's maker	Amazon Web Services Regions in the EU	No
Microsoft Ireland Operations Limited, Dublin	Language models (Azure OpenAI, EU region); the system picks the model for each task	Questions, typed or spoken, and passages found while the answer is written, with the model sorting the topic for the team reports in the same step; on a written instruction, the contents of the test set, to remove the names; not used for training	An Azure region in the EU	No

For the team reports the language model that writes the answer sorts the conversation by topic in the same step, in the EU, or on your own servers inside your network. No person reads along, and the model keeps nothing. The sorting stays in the environment and is deleted with

the conversation.

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 (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).

The parent companies of Amazon Web Services and Microsoft, Amazon.com, Inc. and Microsoft Corporation, are American and both are listed under the EU-U.S. Data Privacy Framework. Our privacy statement explains what that means.

When Inora runs for an organisation elsewhere, on its own servers or outside the EU, its data processing agreement names the suppliers and regions of that deployment.

For our own work

These services support Axiomatic as a company. They never receive data from Inora, so they are not sub-processors in the sense of the data processing agreement. We list them because they process personal data of website visitors and of people who contact us.

Processor	Service	Data	Location
Amazon Web Services EMEA SARL, Luxembourg	Hosting of the website axiomatic.digital (Amazon S3 and Amazon CloudFront)	Technical request data: IP address, page, time, browser	Files in the Europe (Ireland) Region; delivered through CloudFront's global network
Amazon Web Services EMEA SARL, Luxembourg	The AI scan: storage of the answers sent (Amazon DynamoDB), their processing (AWS Lambda) and the email to us (Amazon SES)	Answers, result, language, time and the email address if given	Europe (Ireland) Region
Google Cloud EMEA Limited, Dublin, Ireland	Email, documents and calendar (Google Workspace)	Correspondence and contact details. Notices name the kinds of data and the number of people affected, never data from Inora.	Google's data centres, including outside the EU

Processor	Service	Data	Location
PostHog, Inc., United States	Web analytics and recordings of visits to the website	Pages viewed, clicks, a recording of the visit including what is typed into forms, where the visitor came from, IP address and browser; a copy of the AI scan sent; after a form or a personal link name, email address, role and organisation	PostHog's EU cloud, in Germany
Intercom R&D Unlimited Company, Ireland	The chat on the website	IP address, browser, the page viewed, the conversation; after a form name and email address	United States
IPinfo, Inc., United States	The organisation behind an IP address	The IP address only	United States

PostHog, Intercom and IPinfo never receive data from Inora; they serve only the website, as our privacy statement describes. The US parent companies, Amazon.com, Inc. and Google LLC, and PostHog, Inc. and Intercom, Inc. are listed under the EU-U.S. Data Privacy Framework.

Changes

We announce a new or replacement sub-processor for Inora by email to each customer's contact, at least 30 days before it starts processing. A customer can object within that period. We update this list, and the date at the top, at the same time.

Questions: privacy@axiomatic.digital.

AXIOMATIC

Privacy pack

Inora, for the data protection officer

This pack follows the data processing agreement, the sub-processors list version 1.6, the security overview version 1.4 and the control matrix version 1.3, and the privacy statement. Where they differ, the articles of the signed data processing agreement prevail. You receive the data processing agreement with the proposal.

Version 1.16, 11 November 2026

1. What this pack settles

This pack is for the data protection officer (DPO) or privacy officer of a care organisation assessing Inora. It answers one question: does our data stay within the EU? Yes, your data stays within the EU.

What stands here was filled in by Axiomatic: the description of the processing, the purposes, the facts for the legal basis, the risks with their measures and the DPIA, heading by heading. This pack is Inora's one DPIA document, and it is public. What remains yours is set apart each time under **Your part**: the legal basis, the scale, the weighing of risks for your organisation and your own measures.

2. The processing described

2.1 Roles

Party	Role	Article	What it does
Your organisation	Controller	Art. 4(7) GDPR	Decides what Inora is for, which sources it holds, who works with it and how long conversations stay. Sets the legal basis, carries out the DPIA, reports breaches to the Dutch Data Protection Authority.
Axiomatic B.V., Delft (KvK 97816825)	Processor	Art. 28 GDPR	Builds, implements and runs Inora, only on your documented instructions. Answers to you in full for every sub-processor.
Amazon Web Services EMEA SARL, Luxembourg	Sub-processor	Art. 28(4) GDPR	Hosting in the Europe (Ireland) Region; the language and embedding models through Amazon Bedrock on the EU inference profile. Bound by duties no lighter than Axiomatic's.
Microsoft Ireland Operations Limited, Dublin	Sub-processor	Art. 28(4) GDPR	Language models through Azure OpenAI in the EU region; the system picks the model. Bound by duties no lighter than Axiomatic's.

One party builds, implements and runs Inora. There is no implementation partner, and Inora has no sub-processors other than these two.

The sub-processors' parents are American: Amazon.com, Inc. (Seattle) and Microsoft Corporation (Redmond). Both are listed under the EU-U.S. Data Privacy Framework. Axiomatic transfers no personal data outside the EU. Storage in the EU does not rule out a request from a foreign authority; see §5, risk R4.

2.2 The record of processing

Below is your record (Art. 30(1) GDPR), filled in from the record Axiomatic keeps as processor (Art. 30(2) GDPR). The general purpose: to give care workers answers from the organisation's own sources, and to draft reports in its format. Each processing below states its own purpose, and no other.

- **Processor:** Axiomatic B.V., Delft (KvK 97816825); data protection officer: an external DPO, reachable at fg@axiomatic.digital (Art. 30(2)(a) GDPR).
- **Recipients:** Axiomatic B.V. (processor); Amazon Web Services EMEA SARL and Microsoft Ireland Operations Limited (sub-processors); per team the team lead and the works council.
- **Security:** annex 2 to the data processing agreement.

No.	Data	Whose	What for	Where	How long	Legal basis
P1	Documents: protocols, guidelines, work agreements, the quality handbook, with names of authors and owners	Staff, as author or owner	Searching, and showing as a source	Own storage and search index, Europe (Ireland); embedding through Amazon Bedrock in the EU	As long as you keep the document; out of backups within 30 days	Art. 6 GDPR: for you to fill in
P2	Questions, typed or spoken, answers and reports (SBAR, SOAP); may hold clients' health data	Staff; the clients they ask about	Answers from your sources, reports in your format; per conversation the topic sorted for the team reports, built in	Europe (Ireland); the model in the EU through Amazon Bedrock or Azure OpenAI	90 days, or the period you set; a conversation the function in annex 3 asked for, until the investigation is complete.	Art. 6 GDPR; Art. 9(2)(h) GDPR with Art. 30(3)(a) UAVG: for you to fill in
P3	Accounts: name, work email, a unique identifier and groups from your identity provider, through single sign-on and SCIM	Staff with access	Signing in, access by role	Europe (Ireland)	While access lasts, plus 30 days	Art. 6 GDPR: for you to fill in
P4	Logs: sign-ins, admin actions, IP addresses, times, every access by Axiomatic. Record access is under P11	Your staff and Axiomatic's	Security, incident investigation, accountability; on request you receive 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	Europe (Ireland)	12 months	Art. 6 GDPR: for you to fill in
P5	Support and implementation: only the documents you ask Axiomatic to look at; a staff conversation only under DPA art. 5.5; no copies outside your environment	Staff; the clients they ask about	Solving issues, guiding the implementation	Europe (Ireland), in your own environment	The period of the processing concerned	The basis of that processing, with Art. 9(2)(h) GDPR with Art. 30(3)(a) UAVG, where needed: for you to fill in
P6	Service measure-ments: numbers of questions and response times per user, without content or names	Staff with access	Only to run your own environment and fix problems in it; never to you per worker	Europe (Ireland)	Per user 30 days, after that only totalled per team of at least five people	Art. 6 GDPR: for you to fill in

No.	Data	Whose	What for	Where	How long	Legal basis
P7	Competence record in Inora Matrix, your competence register: per worker the reserved and high-risk procedures under your training policy, with the procedure, the protocol with its version, the date, on whose instruction and who signed off the practical assessment, kept current from what the worker reports doing; their questions to Inora never count; never the content of a conversation, a score or a usage figure	Staff, by name	Only the competence record the inspectorate expects (Wkkgz, Wet BIG); in the pilot a preview for the participating team, until the works council consents	Europe (Ireland)	In Inora for as long as the worker works for you, plus 30 days; in those 30 days you export it to your own personnel file, where your own term applies	Art. 6 GDPR: for you to fill in
P8	Test set: questions from your organisation, and answers a member of staff or a check flagged with their question, stripped of the names of clients and staff by a language model in the EU; no person reads a question or answer in it; only on your written instruction, after the works council's consent where you have one	Staff; the clients they asked about	To test every new version of Inora before it goes live in your environment	Europe (Ireland)	Until you withdraw the instruction, at the latest until the end of the agreement; then deleted within 30 days	Art. 6 GDPR; Art. 9(2)(h) GDPR with Art. 30(3)(a) UAVG: for you to fill in
P9	Answer record: per answer the sources with their versions, the check it passed and the date, and a reference the member of staff sees with the answer; never who asked, the time, the ward, the question or the answer	Staff and clients, only so far as identifiable	Accounting for what an answer rested on, for an incident or a complaint	Europe (Ireland), at Axiomatic; never at the organisation	2 years; then out of backups within 30 days	Art. 6 GDPR: for you to fill in

No.	Data	Whose	What for	Where	How long	Legal basis
P10	Record data, once Inora reads the record, through a connection or the user's own login: what Inora reads from the client record for the task under way, a question, preparing a visit, a review, a rule or signal, at night too; no second record	The clients; the staff in whose name the work runs	Doing the task, with the rights of whoever does the work	Europe (Ireland); the model in the EU, through Amazon Bedrock or Azure OpenAI	The period in your data processing agreement; what remains falls under P2	Art. 6 GDPR; Art. 9(2)(h) GDPR with Art. 30(3)(a) UAVG: for you to fill in
P11	Record log, once Inora reads the record, through a connection or the user's own login: per step what Inora did, on whose behalf, for which client and with what result; never what anyone asks. The EHR keeps its own log	Staff; the clients concerned	Checking record access, set up to NEN 7513; open to the function you appoint, per client or in an investi-gation, never as a figure about one member of staff	Europe (Ireland)	The period in your data processing agreement	Art. 6 GDPR; Art. 9(2)(h) GDPR with Art. 30(3)(a) UAVG: for you to fill in

P1 to P9 follow the order and numbers of annex 1 to the data processing agreement. The privacy statement counts twelve kinds of data: these eleven and, as its part 10, the usage research, for which Axiomatic is itself the controller and which is therefore not in your register; P10 and P11 are parts 11 and 12 there. Backups: daily, encrypted, kept 30 days, in the Europe (Ireland) Region.

The competence record (P7) is your organisation's record, the one the inspectorate expects (Wkkgz, Wet BIG). Axiomatic keeps it in Inora as processor, on your instruction; it serves no other purpose. The worker sees their own competence record in Inora and can ask for a copy to take with them: that is their right of access (Art. 15 GDPR), which your organisation answers and Axiomatic helps with.

The answer record (P9) stays with Axiomatic and is in no screen of your organisation. You receive it on a written request from the function you name in annex 3, for an incident or a complaint, and never who asked.

After the agreement ends you choose return or deletion. Up to and including day 30 the data stays available for return; by day 30 it is gone from active systems, logs and search index included; by day 60 from backups. On request we confirm deletion in writing.

2.3 Data subjects and recipients

- **Data subjects:** your organisation's staff (users, authors and owners of documents) and the clients staff ask about.
- **Recipients:** two sub-processors, both in the EU: Amazon Web Services EMEA SARL (hosting, Amazon Bedrock) and Microsoft Ireland Operations Limited (Azure OpenAI). No one else. We sell nothing, share nothing with other customers and combine nothing. Only the anonymous counts from the usage research does Axiomatic, as controller, total over at least five organisations (privacy statement, item 10).
- **Transfers outside the EEA:** none. Processing outside the EU first requires a written amendment to the data processing agreement and a basis under Chapter V GDPR.

3. Purposes

Inora processes personal data for one general purpose: to give care workers answers from the organisation's own sources and to draft reports in its format. Processings P3 to P9 serve that purpose: signing in, security, support, running your environment, the competence record the inspectorate expects, only on your written instruction the test set with which we test every new version before it goes live in your environment, and the answer record that sets down what an answer rested on. Each of the organisation's sources is marked in the answer, the passage is one tap away, and when the answer is not in the sources, Inora says so.

Axiomatic does not use the data for its own purposes, except the anonymous counts of the usage research, for which Axiomatic is the controller itself (privacy statement, part 10). Axiomatic trains no model on the data and lets no sub-processor do so, and does not combine your organisation's data with another's; only the anonymous counts of the usage research are added up, across at least five organisations. Inora does not diagnose or decide on treatment: the professional decides. Inora supports triage and never triages itself; its intended use keeps it outside the medical device rules.

Your part. Confirm this is your purpose, for each team and location Inora reaches.

4. Legal basis, necessity and proportionality

4.1 The legal basis

The legal basis is your organisation's. For each processing it sets a ground under Article 6 GDPR. Health data also needs an exception to the prohibition in Article 9 GDPR: Article 9(2)(h) GDPR with Article 30(3)(a) UAVG may apply to necessary processing for treatment, care or the management of the institution. It does not cover every use automatically; you assess necessity and professional confidentiality.

What the law asks of us as processor for health data: confidentiality from everyone who can reach the data. Everyone at Axiomatic has signed a confidentiality agreement, and everyone with access to production holds a VOG (Art. 9(3) GDPR; Art. 30(4) UAVG).

4.2 Minimal data

- **Everything typed or spoken counts as health data** and is protected as such.
- **No second client file.** Inora keeps no file beside yours.
- **No BSN.** Inora never asks for a citizen service number.
- **No passwords with single sign-on.** Sign-in runs through your own identity provider (OpenID Connect or SAML). With single sign-on Inora stores no passwords.
- **Only what your single sign-on already holds:** name, work email, a unique identifier and groups.
- **Short retention:** conversations 90 days by default; a longer term you weigh in this DPIA.

4.3 Proportionality and alternatives

The alternative to Inora is what happens now: searching folders or the intranet, calling the colleague who knows, or not knowing. Those alternatives process less data, but leave the care worker without the agreement in force at the moment of care, or spread the same client details over phone and chat with no record.

Your part. Set the legal basis per processing (P1 to P11), and weigh it against the alternatives for your organisation.

5. Risks to data subjects

Each risk with its likelihood and impact without measures, the measure and the residual risk as Axiomatic assesses it. Your organisation weighs them for its own teams and clients.

No.	Risk	Likelihood	Impact	Measure	Residual
R1	Clients' health data in typed or spoken text, read by someone who may not	Medium	High	Everything typed or spoken counts as health data; TLS 1.2 or higher, AES-256 at rest; an environment per organisation; sign-in through your identity provider with single sign-on, a session ends within eight hours; no BSN, no second file; kept 90 days	Low
R2	Watching staff: questions or pace used against a care worker	Medium	High	The four rules of §7: no screen of conversations in the organisation; reports per team of at least five, the topic sorted by the language model that writes the answer, without names; unanswered questions as a topic, without a name or the care worker's words; access by Axiomatic only on a written request, for an incident or a complaint, logged, the care worker told; in a failure only the logs and the answer record, never a conversation. No score, no assessment, no emotion recognition (AI Act Art. 5(1)(f)); one member of staff's sign-in times and IP addresses never to the organisation. Service measurements and the competence record: R6 and R7	Low
R3	A wrong answer with consequences for the client	Low	High	Every answer rests on the organisation's sources, each source marked, the passage one tap away; Inora says so when the answer is not in the sources; the professional decides	Low
R4	A foreign authority's request to a sub-processor's US parent	Low	High	Processing and storage only in the EU, by AWS EMEA SARL and Microsoft Ireland Operations Limited; encryption; notice to you before any disclosure, unless the law forbids it; objection to any request without a valid basis; a foreign order is no ground for transfer (Art. 48 GDPR)	Low, not nil
R5	A data breach	Low	High	Built to NEN 7510 and ISO 27001; only the engineers who build Inora reach production, named in the processing agreement, with a personal account, MFA and a VOG, every access logged; monitoring; critical patches within 72 hours; notice to you no later than 24 hours after we become aware	Low
R6	Service measurements per user used as a performance measure of one member of staff	Low	High	Per user 30 days, then only totalled per team of at least five people; only to run the environment; never per member of staff to the organisation	Low
R7	A wrong or missing entry in the competence record, with consequences for the worker's work	Low	High	Only the procedure, the protocol with its version, the date and on whose instruction; they see their own record in Inora and have an error corrected (Art. 16 GDPR); never a score or a usage figure	Low

No.	Risk	Likelihood	Impact	Measure	Residual
R8	A question in the test set traced to a client or member of staff, or kept longer than needed	Low	Medium	Only on your written instruction, after the works council's consent where you have one; names removed by a language model; no person reads a question or answer in the test set, testing is automated; only to test new versions; at the latest until the end of the agreement, gone within 30 days of withdrawal	Low
R9	The answer record traced to whoever asked	Low	Medium	No name, time, ward, question or answer; it stays with Axiomatic; only through DPA art. 5.5 and 5.6, for an incident or a complaint	Low

Your part. The weighing for your organisation: which teams, which clients, which residual risks you accept. Whether prior consultation is needed is in §6.7. Axiomatic helps.

6. The DPIA, heading by heading

Article 35(7) GDPR names what a DPIA must at least contain; Article 35(9) asks for the views of data subjects, Article 36 for the weighing on prior consultation. Per heading: what Axiomatic filled in, what is yours and where it is backed. This pack is Inora's one DPIA document, public; Axiomatic provides it free of charge.

6.1 Systematic description (Art. 35(7)(a))

Filled in by Axiomatic. Nine processings, two more once Inora reads the record, through a connection or the user's own login. In the order of DPA annex 1: documents, questions with answers and reports, accounts from your identity provider, the logs, support and implementation, service measurements, the competence record, the test set and the answer record. Data subjects: your staff and the clients they ask about. Recipients: two sub-processors, both in the EU: Amazon Web Services EMEA SARL (hosting, Amazon Bedrock) and Microsoft Ireland Operations Limited (Azure OpenAI). See §2.

Your part. The scale: how many staff, which teams and locations, how many sources.

Backed in. This pack §2; Sub-processors version 1.6.

6.2 Purposes (Art. 35(7)(a))

Filled in by Axiomatic. Answers from the organisation's own sources and reports in its format, with per processing the purpose in the record, and no other. No training, never combined with another organisation. See §3.

Your part. Confirm this is your purpose, for each team Inora reaches.

Backed in. DPA cl. 3.1, 3.3 and 3.9; this pack §3.

6.3 Necessity and proportionality (Art. 35(7)(b))

Filled in by Axiomatic. No BSN, no second client file. With single sign-on no passwords and only what your single sign-on already holds. Conversations 90 days by default; a longer term you weigh in this DPIA. See §4.

Your part. Set the legal basis, and weigh it against what happens now: searching the intranet, calling a colleague, not knowing.

Backed in. This pack §4, Legal bases.

6.4 Risks to data subjects (Art. 35(7)(c))

Filled in by Axiomatic. Nine risks, each with likelihood, impact and measure: health data in typed or spoken text, watching staff, a wrong answer, a request from a foreign authority, a data breach, service measurements used as a performance measure, an error in the competence record, a question in the test set (only on your instruction) traced or kept too long, and the answer record traced to whoever asked. See §5.

Your part. The weighing for your organisation: which teams, which clients, which residual risks you accept.

Backed in. This pack §5, the risk table.

6.5 Measures (Art. 35(7)(d))

Filled in by Axiomatic. Built to NEN 7510 and ISO 27001. An environment per organisation (its own database, document storage and search index), sign-in through your identity provider with single sign-on, TLS 1.2 or higher and AES-256, only the engineers who build Inora reach production, named in the processing agreement, with MFA and a VOG, every access logged, logs kept 12 months. Backups daily, encrypted, kept 30 days, in the Europe (Ireland) Region, with a restore test every quarter. Breach notice no later than 24 hours after we become aware.

Your part. Your own measures: which groups get access, who manages sources, and what you ask staff about what they type.

Backed in. Security overview version 1.4; the control matrix, the basis for your statement of applicability.

6.6 Views of data subjects (Art. 35(9))

Filled in by Axiomatic. Your staff speak through the works council: its consent (art. 27 WOR) is their view. The consent request is ready, with the four rules on conversations from §7.

Your part. Ask for the consent and record it, and hear the client council where it fits.

Backed in. The Works council page (axiomatic.digital/en/products/evaluate/works-council); the consent request.

6.7 Prior consultation (Art. 36)

Filled in by Axiomatic. Not needed when the measures of §5 and §6.5 remove the high risk. Our estimate of the residual risk stands per risk in the risk table of §5.

Your part. Your DPO weighs the residual risk and records the weighing. If a high risk remains, you consult the Dutch Data Protection Authority before the start.

Backed in. This pack §5

7. Staff conversations: four rules

What a member of staff asks Inora, no one in the organisation reads; Axiomatic only by the rules below. The four rules, each with where it is bound. You can hand this chapter to the works council as it is.

1. **No one in the organisation reads a conversation, management included.** No administrator, manager or board member can open a care worker's questions and answers in Inora; no screen for it exists. *Bound in:* privacy statement, Staff conversations
2. **Reports cover teams of at least five people.** The monthly report shows per team the topics staff ask about, with counts, never per person. Per team to the team lead and the works council; the board and quality receive the sum across all teams. The topic is set together with the answer, without names; no person reads along. Inora assesses no one and gives no one a score. *Bound in:* privacy statement, Staff conversations

3. **A question without an answer goes as a topic, without a name and without the asker's words, to whoever owns the subject,** with a count and per protocol, so the source can be completed. For example: *Insulin pen: shelf life outside the fridge · 2×. Bound in:* privacy statement, Staff conversations
4. **Axiomatic reads a conversation only on a written request, for an incident or a complaint.** Axiomatic reads a conversation only on a written request from the function you name in annex 3 of the DPA, such as your data protection officer, 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. 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. *Bound in:* privacy statement, Staff conversations

DPA art. 5.6, verbatim: *"5.6 The Processor gives the Controller no figure, score or assessment about a single worker and none of the content of their conversations. Nor does the Processor give it the sign-in times or IP addresses of a single worker; on request the logging goes to it totalled per team of at least five people and per day, and a day with fewer than five sign-ins shows as '<5' (Annex 1, item 4). Usage reports cover teams of at least five people only: per team to the team lead and the works council; the board and quality receive only the sum across all teams. For those reports 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 (Annex 1, item 2). These reports are part of Inora and need no separate instruction. A question without an answer goes as a topic, without a name and without the asker's words, to whoever owns the subject. A topic asked once goes in only when it comes a second time; after three months it goes only into the sum across all teams. Besides what the member of staff personally sends, such as their report on their approval or their incident report, only the competence record the inspectorate expects the Controller to keep (Wkkgz, Wet BIG), for reserved and high-risk procedures under its training policy, goes to the Controller per worker. 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. Only the Controller's team lead and training department see the competence record, and the member of staff themselves. The worker sees their own competence record in Inora and receives a copy on request (Article 15 GDPR; Article 7). The Processor answers a request from a data subject (Article 15 GDPR) by the route of clause 7, with only what that request asks, never as access for management. The Processor answers a legal demand by the route of clauses 3.7 and 6.6, with only what the demand asks; then too the Processor logs the access and tells the member of staff that their conversation was read, unless the law forbids it. Inora infers no emotions or mood of a member of staff (AI Act, Article 5(1)(f)). A wrong answer is a finding about Inora and the source, never about the member of staff who came across it. For every answer the Processor keeps an answer record with the sources and their versions, the model, the check it passed, the date and a reference the member of staff sees with the answer, without who asked, the time of day, the ward or the content of question and answer. It stays with the Processor; the Controller receives it only by the route of clause 5.5 (Annex 1, item 9)."*

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 is P7 in §2.2; the answer record (P9) stays with Axiomatic.

8. Data breaches: who does what

Moment	Who	What
Hour 0	Axiomatic	Sees a data breach, or suspects one.
Within 24 hours	Axiomatic	Reports it to your contact in DPA annex 3, with its nature, the people affected, the consequences, the measures and a contact. The 24 hours are a maximum, not a waiting period. Notices name the kinds of data and the number of people affected, never data from Inora.
Within 72 hours of our notice	Your organisation	Reports it to the Dutch Data Protection Authority where it must be reported (Art. 33 GDPR), and to the people affected where needed (Art. 34 GDPR). Your 72 hours start when we notify you; our 24 hours come before them. Axiomatic does not report to the authority itself.
Within 10 working days	Axiomatic	A written report of cause, consequences and measures.

9. Sub-processors

For an organisation in the EU, Inora has two sub-processors. Amazon Web Services EMEA SARL: hosting in Europe (Ireland) and the model through Amazon Bedrock on the EU inference profile. Microsoft Ireland Operations Limited: Language models through Azure OpenAI in the EU region; the system picks the model. 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 sorting stays in the environment and is deleted with the conversation. Neither trains a model on your data. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker. 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, Abuse monitoring).

A new or replacement sub-processor we announce by email at least 30 days ahead. You can object within that period; until it is resolved, the new sub-processor processes nothing of yours. If we find no solution, you end that part with no fee and get back what you paid in advance.

10. What you receive from us

- This privacy pack, with the DPIA pre-filled: Inora's one DPIA document, public.
- The list of sub-processors, version 1.6.
- The security overview version 1.4 and the control matrix version 1.3, the basis for your statement of applicability.
- The privacy statement, at axiomatic.digital/en/trust/privacy.

Our data protection officer is an external DPO, reachable at fg@axiomatic.digital and notified to the Dutch Data Protection Authority. Questions about this pack: privacy@axiomatic.digital.

AXIOMATIC

Pack for the works council

Inora and staff data. What goes to the organisation, what never does, and where it stands.

Version 1.9, 11 November 2026

This pack is for the members and the secretary of the works council of a care organisation that intends to introduce Inora. It answers one question: do our staff's conversations stay private? Yes, your staff's conversations stay private. Below is how, what does go to the organisation, and in which document each rule stands, so the council consents on terms, not promises.

The consent request itself, with the information letter, is a separate document: *Information letter and model consent request*, version 1.7 of 7 November 2026.

1. What Inora is

Inora is the care organisation's knowledge system, built on its own knowledge. They ask a question in plain language and get an answer from the organisation's own protocols, work agreements and guidelines, with the source attached. Inora readies the report in the organisation's format; the care worker reads and signs, and only on that approval does Inora file it in the client record; Inora acts on that person's behalf, never with more rights than they have. The professional checks and decides.

That takes three steps out of the shift: finding out how it is done here, doing it and logging it, and writing it up.

Inora is made by Axiomatic B.V. in Delft and built to NEN 7510 and ISO 27001. Data stays in the EU or on the organisation's own servers; no model trains on it. Staff sign in with their own organisation's account, through single sign-on.

2. Why the council has the right of consent

Article 27(1) of the Works Councils Act (WOR) gives the works council the right of consent over:

- **under (k):** a scheme for the processing and protection of the personal data of the people working in the enterprise;
- **under (l):** a scheme for facilities aimed at or suited to observing or checking the attendance, conduct or performance of the people working in the enterprise.

Inora processes staff data and records work, so both apply. The board puts the decision in writing, with the reasons and the consequences for staff; the council decides only after at least one consultation meeting and gives its decision in writing, with reasons (article 27(2)). A decision taken without consent is null if the council invokes that in writing, within one month of the board telling it that it is carrying the decision out, or of that becoming apparent to the council (article 27(5)).

Source: Works Councils Act, article 27 (Dutch).

3. The line

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 line is not a setting; it is in Inora, and no administrator, manager or board member can change it.

	What Inora knows about a care worker's work	What the line does with it
Rule 1	The care worker's conversations	Stops. No one in the organisation opens their conversations, management included.
Rule 2	How often, how fast and when the care worker works	Stops. No figure about one member of staff, for anyone in the organisation.
Rule 3	A judgement of the care worker's work	Stops. Inora assesses no one and gives no one a score.
Rule 4	The care worker's mood	Stops. Inora infers no emotions, from voice or face.

	What Inora knows about a care worker's work	What the line does with it
Rule 5	What Axiomatic reads on request	Stops. 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. 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.
Rule 6	What the care worker's team asks about	Crosses, per team of five or more: the monthly report, without a single name. Per team to the team lead and the works council; the board and quality receive the sum across all teams.
Rule 7	A question with no answer	Crosses. A question with no answer goes as a topic, without a name and without the asker's words, to the owner, pooled per protocol, so the source gets completed.
Rule 8	A wrong answer	Crosses, as a finding about Inora and the source, never about whoever came across it.
Rule 9	A reserved or high-risk procedure	Crosses, by name: the competence record, with the procedure, the protocol with its version, the date and on whose instruction. The care worker sees it themselves in Inora.

Outside the line, because the organisation switches it on itself and only if the council consents (condition 11):

- **Test set.** Questions from the organisation and flagged answers with their question, without names, to test every new version of Inora; no person reads a question or answer for it. Only on the organisation's written instruction, after the works council's consent.

4. What management sees: the monthly report per team

Per team to the team lead and the works council; the board and quality receive the sum across all teams. The topic is set together with the answer, without names; no person reads along. Per team of at least five people the monthly report holds:

- what was asked about, per subject, with the team's count together;
- which topics found no answer yet, with a count, as their owner receives them: rewritten without identifying detail, without a name and without the asker's words, pooled per protocol. A topic asked once goes in only when it comes a second time; after three months it goes only into the sum across all teams;
- which gaps in the work agreements were closed;
- how much time Inora gave the team back.

It never holds: a name, a question as someone typed it, a figure per person, one member of staff's times or pace, a score. A team of fewer than five people gets no report of its own, so no one in it can be recognised.

Example, Zorggroep Voorbeeld, Heuvelland-Oost district team (11 members of staff), October 2026

Part	Content
What the team asked about	Wound care 41, Medication 33, Reporting 28, Catheter care 17, Other subjects 24 (143 questions)
No answer yet	4: Insulin pen: shelf life outside the fridge · 2× (to medication policy); Replacing a urinary catheter: who may do it · 2× (to reserved procedures). Without a name and without the asker's words
Gaps closed	2 work agreements completed
Time given back	14 hours, for the whole team
Heuvelland night shift (4 members of staff)	No report of its own

The figures are the example's; an organisation's real report is confidential.

5. The competence record

Whoever performs a reserved procedure on the instruction of an independently authorised professional, such as a doctor, must be competent to do so and follows their directions (Wet BIG, articles 35 and 38). A subcutaneous insulin injection and inserting a catheter are such procedures. The inspectorate expects the organisation to show that competence, for high-risk procedures too. Today that is often kept on paper or in a training system, and often after the fact.

That competence record, besides what the care worker sends themselves the only thing by name that goes to the organisation (section 3), covers reserved and high-risk procedures under the organisation's training policy. It is the organisation's own record; Axiomatic keeps it in Inora as processor, on its instruction. Inora records it from what the care worker did; what they asked or read does not go with it. 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. Inora Matrix is the organisation's competence register for it: per role it lists the procedures the training policy asks for, the assessor signs off the practical assessment in the same report flow, and from then on the register stays current with the procedures the member of staff reports doing themselves, with the protocol and the version that applied. The care worker's questions to Inora never count, not even as evidence of competence. In the pilot it is a preview for the participating team and staff take part voluntarily; it becomes the official register only after the works council consents.

An example.

Field	Content
Care worker	Sanne de Wit, senior care assistant
Procedure	Subcutaneous insulin injection, a reserved procedure
Protocol	Insulin administration, version 6
Date	14 October 2026
On whose instruction	The client's attending physician

Goes to the organisation	Never goes there
Who, which procedure and which protocol, with its version	What she asked or read
The date, and on whose instruction	How often she uses Inora
	How long she took
	A score or a judgement

Retention. In Inora for as long as the care worker 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.

Who sees it. The care worker themselves: their own competence record, always, in Inora. They can ask for a copy to take with them: that is their right of access (article 15 GDPR), which the organisation answers and Axiomatic helps with. The team lead and training: the competence

record, to know who may perform which procedure; they had to know that already. No one else.

Why it serves the care worker. Their competence is recorded at the moment itself, not afterwards, with the protocol and the version in force, and they see for themselves what it says about them. Proof of their craft, not a yardstick.

Source: Wet BIG, articles 35 and 38 (Dutch).

6. The rules in writing

Each rule of the line stands word for word in a document the council can cite in its decision. The board receives the data processing agreement with Axiomatic's proposal; the council asks the board for it.

Rule 1. No one in the organisation reads a care worker's conversation.

- Data processing agreement, art. 5.5: "No administrator, manager or board member of the Controller can open a member of staff's conversations in Inora."
- Privacy statement, Staff conversations: "No one in the organisation reads a conversation, management included."

Rule 2. No one in the organisation gets a figure about one member of staff.

- Inora and the EU AI Act, What Inora never does: "Figures on use cover only teams of at least five people, never one member of staff, and no one gets a score."
- Data processing agreement, art. 3.4: "The Controller instructs the Processor to use Service Metrics only to operate its Environment and resolve problems within it."
- Data processing agreement, art. 5.6: "The Processor gives the Controller no figure, score or assessment about a single worker and none of the content of their conversations."

Rule 3. Inora assesses no one.

- Inora and the EU AI Act, What Inora never does: "It does not evaluate staff or take decisions about their work."
- Privacy statement, Staff conversations: "Inora assesses no one and gives no one a score."

Rule 4. No emotion recognition.

- Data processing agreement, art. 5.6: “Inora infers no emotions or mood of a member of staff (AI Act, Article 5(1)(f)).”
- Inora and the EU AI Act, What Inora never does: “It infers no emotions or mood of staff, from voice or face. Article 5(1)(f) prohibits that.”

Rule 5. Axiomatic reads a conversation only on a written request, for an incident or a complaint, and never in an outage; the requester gets a finding about Inora, never what the member of staff asked. The member of staff is told of a legal demand, unless the law forbids it.

- Data processing agreement, art. 5.5: “The Processor reads a conversation between a member of the Controller’s staff and Inora only on a written request from the function the Controller names for it in Annex 3, such as its data protection officer, and for the purpose the request states: an incident or a complaint. The Processor reads only what that purpose needs, logs every access and tells the member of staff that their conversation was read. In a failure or a security incident the Processor examines the system logs and the answer record, with the sources, their versions and the checks, and never a conversation.”
- Data processing agreement, art. 5.6: “The Processor answers a legal demand by the route of clauses 3.7 and 6.6, with only what the demand asks; then too the Processor logs the access and tells the member of staff that their conversation was read, unless the law forbids it.”
- Privacy statement, Staff conversations: “Whoever made the request gets a finding about Inora, never what the member of staff asked or read.”

Rule 6. Reports only per team of five or more.

- Data processing agreement, art. 5.6: “Usage reports cover teams of at least five people only: per team to the team lead and the works council; the board and quality receive only the sum across all teams. For those reports 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 (Annex 1, item 2). These reports are part of Inora and need no separate instruction.”
- Privacy statement, Staff conversations: “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.”

Rule 7. A question with no answer goes as a topic, without a name and without the asker’s words, to the owner.

- Data processing agreement, art. 5.6: “A question without an answer goes as a topic, without a name and without the asker’s words, to whoever owns the subject. A topic asked once goes in only when it comes a second time; after three months it goes only into the sum across all teams.”
- Privacy statement, Staff conversations: “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.”

Rule 8. A failure is a finding about the system.

- Data processing agreement, art. 5.6: “A wrong answer is a finding about Inora and the source, never about the member of staff who came across it.”
- Trust, No one is blamed: “Without blame: in the source, the model, the software around it, the configuration and our own way of working. No finding names whoever came across the failure.”
- Consent request, condition 8: “A wrong answer is a finding about Inora and the source, never about the member of staff who came across it.”

Rule 9. What a care worker asks Inora never reaches the organisation; by name only the competence record goes.

- Record log: the record log shows, once Inora reads the record, through a connection or the user’s own login, per step what Inora did and on whose behalf. The function the organisation appoints sees it only on written request, per client or in an investigation, to check record access; it is no figure about a member of staff and never holds what anyone asks.
- Data processing agreement, art. 5.6: “Besides what the member of staff sends themselves, such as their report on their approval or their incident report, only the competence record the inspectorate expects the Controller to keep (Wkkgz, Wet BIG), for reserved and high-risk procedures under its training policy, goes to the Controller per worker. 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. Only the Controller’s team lead and training department see the competence record, and the member of staff themselves. The worker sees their own competence record in Inora and receives a copy on request (Article 15 GDPR; Article 7).”

- Privacy statement, Staff conversations: “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.”
- Consent request, condition 9: “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). The care worker’s questions to Inora never count, not even as evidence of competence.”

The test set: only with the council’s consent.

- Data processing agreement, art. 3.8: “No Staff Member of the Processor reads a question or answer in the test set; testing a new version is automated.”
- Consent request, condition 11: “We switch on the test set only if you consent to it separately below.”

7. Retention and logs

Data	What for	How long, and what the organisation receives
Documents: names and functions of staff as author or owner	Shown as source	As long as the document stays in Inora
Account: name, work e-mail address, unique code and groups	So that only authorised staff have access	As long as the member of staff has access, and 30 days after
Conversations: questions, answers and drafted reports, and the topic of each conversation, without names	So the member of staff finds their own conversation again, and the topic for the monthly report per team	90 days by default, set by the organisation; no one in the organisation opens them. If the organisation asks Axiomatic, within the retention term, to read a conversation for an incident or a complaint, Axiomatic holds it until the investigation is complete and deletes it within 30 days after; the member of staff is told

Data	What for	How long, and what the organisation receives
Logs: sign-ins, administrative actions and every access by Axiomatic	Keeping the service secure	12 months. On request the organisation receives the logs only totalled per team of at least five people and per day; a day with fewer than five sign-ins shows as ‘<5’; one member of staff’s sign-in times and IP addresses never
Service metrics: numbers of questions and response times per user	Only to run the environment	Per user 30 days, then only totalled per team of at least five people; never per member of staff to the organisation
Test set: questions from the organisation and flagged answers with their question, names removed	Only on the organisation’s written instruction, after the works council’s consent, to test new versions; no person reads a question or answer for it	Until the organisation withdraws the instruction, at the latest until the end of the agreement; then gone within 30 days
Competence record: the procedure, the protocol with its version, the date and on whose instruction	The record the inspectorate expects of the organisation (Wkkgz, Wet BIG)	In Inora for as long as the care worker 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
Answer record: per answer the sources with their versions, the check it passed and the date, and a reference the member of staff sees with the answer; never who asked, the time, the ward, the question or the answer	Accounting for what an answer rested on, for an incident or a complaint	2 years, at Axiomatic. The organisation receives it only on written request, never who asked

Apart from the competence record and what the member of staff sends themselves, nothing from any of these data goes to the organisation per member of staff. In an outage or security incident Axiomatic examines the system logs and the answer record, never a conversation, and reports a finding about the system, naming no care worker. After the agreement ends, everything is deleted from active systems within 30 days and from backups within 60 days, and on request confirmed in writing.

8. What staff gain

The council protects staff, and weighs what they get too. Inora takes three steps out of the shift: finding out how it is done here (the organisation's own protocol, with its source, at the bedside), doing it and logging it, and writing it up (the report is ready before the care worker gets back in the car: Inora readies it, they sign, and it goes into the record on their approval). Care workers say so themselves:

- "Good to check something quickly without having to call anyone. It gives certainty." Care worker, South Limburg, questionnaire report, ZorgConnect Zuid-Limburg, 12 January 2026.
- "It helps me have better conversations with doctors, clients or family and feel safer in my work, even when there is no colleague nearby to ask a question." Nurse, Limburg, De Limburger, 22 April 2026.
- "It confirms what I already know. That gives me peace of mind." Care worker, South Limburg, questionnaire report, ZorgConnect Zuid-Limburg, 12 January 2026.

The time that comes back. It goes back to care: to clients, and to the work that now waits until after the shift. The organisation decides on staffing, not Axiomatic, and Axiomatic never sells Inora as a cut in staff. The model request sets this down as condition 10. A funding application counts in fte saved, as the scheme asks; what the organisation does with that time, the board puts to the council separately.

Works councils of care organisations that work with Inora consented to a request with the same rules, usually in one meeting. "We consented in one meeting. The letter was already there." Works council member, care group.

9. Consent, evaluation and change

The model consent request sets the nine rules of the line down as the conditions of consent, with the terms on the time that comes back as the tenth and the test set as the eleventh: the organisation switches it on only if the council consents. Besides that:

- **When.** The board puts the consent request to you during the pilot: in a pharmacy the pharmacist-owner, in a municipality the management. The council consents after at least one consultation meeting (WOR article 27(2)); without consent no other team follows and Inora Matrix does not become the official competence register. The pilot runs eight weeks; after it the organisation decides which teams follow, and every new purpose comes back to you as a new consent request.

- **Evaluation.** The board evaluates the introduction with the council after the eight-week pilot and every year after, with the monthly report per team and an overview of every access by Axiomatic, without its content.
- **Change.** Every change to the conditions, and every other purpose, comes back to the council as a new request for consent. What management sees per team cannot quietly grow; the terms with Axiomatic change only in writing.
- **If a condition is not kept.** Use outside the conditions is a decision without consent. The council can invoke its nullity in writing, within one month of the board telling it of that use or of it becoming apparent to the council (WOR article 27(5)), and the board stops that use.

10. The documents with this pack

- Privacy statement, with Staff conversations: axiomatic.digital/en/trust/privacy.
- Inora and the EU AI Act, with What Inora never does: axiomatic.digital/en/trust/ai-act.
- Data processing agreement with Axiomatic.
- An example of the monthly report per team (section 4).
- Information letter and model consent request, version 1.7 of 7 November 2026.

AXIOMATIC

Information letter and model consent request

Inora, for the works council. WOR article 27(1)(k) and (l).

Version 1.7, 7 November 2026

This document holds two parts, each on a new page:

1. **The information letter to the works council**: what Inora is, which rules on staff data are built into the system and which clauses bind them.
2. **The model consent request**: the proposed decision the board puts to the works council in writing (WOR article 27(2)), with the conditions on which the council consents before the rollout to more teams after the pilot and before Inora Matrix becomes the official competence register.

Fill in the text between square brackets. Adapt what is different in your organisation; leave the conditions in article 4 of the request as they are, because the consent rests on them.

1. The information letter

[Name of the organisation]
To the works council
[Place], [date]

Subject: information with the request for consent to the introduction of Inora

Dear members of the works council,

We will shortly ask for your consent to the introduction of Inora. Before you decide, this letter gives you everything you need: what Inora is, what it does and does not do with staff data, and in which document each rule stands. You need take nothing on our word.

What Inora is

Inora is our organisation's knowledge system, built on our own knowledge. A care worker asks a question in plain language, at the bedside or in the car, and gets an answer from our own protocols, work agreements and guidelines, with the source attached. Inora readies the report in our own format; the care worker reads and signs, and only on that approval does Inora file it in the client record; Inora acts on that person's behalf, never with more rights than they have. The care worker checks the answer against its source and decides.

That takes three steps out of the shift: finding out how it is done here, doing it and logging it, and writing it up. That work now often happens after the shift.

Inora is made by Axiomatic B.V. in Delft. It is built to NEN 7510 and ISO 27001. Data stays in the European Union, or on our own servers, and no model trains on it. Staff sign in with their own account of our organisation with two-step verification.

Why you have the right of consent

Inora processes staff data: their account, their questions and the answers they received. A scheme for the processing and protection of staff personal data (WOR article 27(1)(k)) and a scheme for facilities suited to observing or checking staff attendance, conduct or performance (under (l)) need your consent. That holds for every system that records data about work, even when it is not meant to watch anyone. You are right to ask.

The line: what goes to the organisation about a member of staff, and what never does

Inora is built around one rule: nothing about an individual care worker goes to the organisation, except what they send themselves and the competence record. 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 line is not a setting an administrator can change; it is in the system.

What never goes to the organisation

- **What the care worker asks and reads.** 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.
- **How often, how fast and when the care worker works.** No one in the organisation gets a figure about one member of staff. Figures on use cover only teams of at least five people.

- **A judgement of the care worker's work.** Inora assesses no one and gives no one a score.
- **The care worker's mood.** Inora infers no emotions or mood, from voice or face. The AI Act prohibits that (article 5(1)(f)).
- **What Axiomatic reads on request.** Axiomatic reads a conversation only on a written request from the function we name for it, such as the data protection officer, 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. 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.

What does go to the organisation, and why that protects staff

- **The monthly report per team.** Per team of at least five people: what was asked about, which topics found no answer yet, with a count, which gaps in the work agreements were closed and how much time Inora gave the team back. No name, no question as someone typed it, no figure per person, no score. The topic is set together with the answer, without names; no person reads along. Per team to the team lead and the works council; the board and quality receive the sum across all teams. A team of fewer than five gets no report of its own.
- **A question with no answer, as a topic.** When the answer is not in our 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 gets completed. The name of whoever asked does not go with it. A topic asked once goes in only when it comes a second time; after three months it goes only into the sum across all teams.
- **A wrong answer, as a finding about the system.** If a member of staff comes across a wrong answer, that is a finding about Inora and the source. No finding names whoever came across the failure.

- **The competence record.** Whoever performs a reserved procedure on the instruction of an independently authorised professional, such as a doctor, must be competent to do so and follows their directions (Wet BIG, articles 35 and 38), and the inspectorate expects us to show that competence, for high-risk procedures too. Inora Matrix is our competence register for it: per role it lists the procedures our training policy asks for, the assessor signs off the practical assessment, and from then on the record stays current with the procedures the member of staff reports doing themselves, with the protocol and the version that applied. The care worker's questions to Inora never count, not even as evidence of competence. It is our own record; Axiomatic keeps it in Inora as processor. It records only the procedure, the protocol with its version, the date, on whose instruction and who signed off the practical assessment, never the content of a conversation, a score or a usage figure. In the pilot it is a preview for the participating team and staff take part voluntarily; it becomes our official register only after your consent. Only our team lead and training department see the competence record, and the member of staff themselves. The member of staff sees their own competence record in Inora and receives a copy on request (article 15 GDPR).

What is kept, and for how long

Data	What for	How long, and what we receive
Documents: names and functions of staff as author or owner	Shown as source	As long as the document stays in Inora
Account: name, work e-mail address, unique code and groups from our identity provider	So that only authorised staff have access	As long as the member of staff has access, and 30 days after
Conversations: questions, answers and drafted reports, and the topic of each conversation, without names	So the member of staff finds their own conversation again, and the topic for the monthly report per team	90 days by default; we set the period. No one in our organisation opens them. If we ask Axiomatic, within the retention term, to read a conversation for an incident or a complaint, Axiomatic holds it until the investigation is complete and deletes it within 30 days after; the member of staff is told
Logs: sign-ins, administrative actions and every access by Axiomatic	Keeping the service secure	12 months. On request we receive the logs only totalled per team of at least five people and per day; a day with fewer than five sign-ins shows as '<5'; one member of staff's sign-in times and IP addresses never

Data	What for	How long, and what we receive
Service metrics: numbers of questions and response times per user	Only to run the environment	Per user 30 days, then only totalled per team of at least five people; never per member of staff to us
Test set: questions from our organisation and flagged answers with their question, without names	Only on our written instruction, after your consent, to test new versions; no person reads a question or answer for it	Until we withdraw the instruction, at the latest until the end of the agreement; then gone within 30 days
Competence record: the procedure, the protocol with its version, the date, on whose instruction and who signed off the practical assessment; never the content of a conversation, a score or a usage figure	The record the inspectorate expects of us (Wkkgz, Wet BIG)	In Inora for as long as the member of staff works for us, plus 30 days; in those 30 days we export it to our own personnel file, where our own term applies
Answer record: per answer the sources with their versions, the check it passed and the date, and a reference the member of staff sees with the answer; never who asked, the time, the ward, the question or the answer	Accounting for what an answer rested on, for an incident or a complaint	2 years, at Axiomatic. We receive it only on written request, never who asked

Apart from the competence record and what the member of staff sends themselves, we receive nothing per member of staff from any of these data. After the agreement ends, everything is deleted from active systems within 30 days and from backups within 60 days, and on request Axiomatic confirms that in writing.

Where each rule stands

Rule	Where it stands
No one in the organisation reads a conversation	Data processing agreement, art. 5.5; Privacy statement, Staff conversations
No one in the organisation gets a figure about one member of staff	Inora and the EU AI Act, What Inora never does.6
No one gets a score	Inora and the EU AI Act, What Inora never does; Privacy statement, Staff conversations

Rule	Where it stands
No emotion recognition	Data processing agreement, art. 5.6; Inora and the EU AI Act, What Inora never does; AI Act, art. 5(1)(f)
Axiomatic reads a conversation only on a written request, never in an outage; the member of staff is told of a legal demand	Data processing agreement, art. 5.4, 5.5 and 5.6; Privacy statement, Staff conversations
Reports only per team of five or more, per team to the team lead and the works council	Data processing agreement, art. 5.6; Privacy statement, Staff conversations
A question with no answer goes as a topic, without a name and without the asker's words	Data processing agreement, art. 5.6; Privacy statement, Staff conversations
A failure is a finding about the system	Data processing agreement, art. 5.6; Trust, When something goes wrong; this request, condition 8
What a care worker asks never reaches the organisation; by name only the competence record	Data processing agreement, art. 5.6; Privacy statement, Staff conversations; this request, condition 9
The time that comes back goes to care	This request, condition 10
Test set only with your consent	Data processing agreement, art. 3.8; this request, condition 11

The pages are at axiomatic.digital/en/trust; we enclose the data processing agreement with Axiomatic.

What we ask of you

We put the request on the next page to you in writing, with the reasons and the consequences for staff. We will discuss it with you at the consultation meeting of [date of the meeting], before the rollout to more teams after the pilot; without your consent no other team follows and Inora Matrix does not become the official competence register. You then decide, and let us know your decision in writing and with reasons (WOR article 27(2)). If you have questions beforehand, we or Axiomatic will answer them, at your meeting or on paper.

Kind regards,

[Name]
[Function]

2. The model consent request

[Name of the organisation], the board
To the works council of [name of the organisation]
[Place], [date]

Subject: request for consent to the introduction of Inora (WOR article 27(1)(k) and (l))

Dear members of the works council,

Under article 27 of the Works Councils Act we ask for your consent to the proposed decision below.

Article 1. The proposed decision. We introduce Inora, starting with an eight-week pilot in [name of the team], from [start date] to [end date]. Taking part in the pilot is voluntary; during the pilot Inora Matrix is a preview for the pilot team. Until you have consented, no other team works with Inora and Inora Matrix does not become the official competence register. After the pilot we decide which teams follow. This decision contains the scheme for the processing and protection of staff personal data in Inora, with the conditions in article 4.

Article 2. The reasons. Care workers look up how it is done here, log what they did and write it up, often after their shift. Inora takes those three steps over, with answers from our own protocols and the source attached. Inora readies the report; the care worker reads and signs, and only on that approval does Inora file it in the client record; Inora acts on that person's behalf, never with more rights than they have. We want to bring administration time down, make the current work agreement reachable at any moment, at night too, and give the time back to the client.

Article 3. The consequences for staff. Staff in the teams that work with Inora sign in with their own account. They ask questions in plain language and check the answer against its source; they decide. No one is required to ask Inora instead of a colleague. Staff receive training at the start. The pilot measures the effect per team, never per person.

Article 4. The conditions. We introduce Inora only on these conditions:

1. No one in the organisation reads a member of staff's conversation with Inora, management included.
2. No one in the organisation gets a figure about one member of staff: not how often, how fast or when they work.
3. Inora assesses no one and gives no one a score.

4. Inora infers no emotions or mood.
5. Axiomatic reads a conversation only on a written request from [function, for example the data protection officer], 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. 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.
6. Reports cover teams of at least five people: per team to the team lead and the works council; the board and quality receive the sum across all teams. A smaller team gets no report of its own. The topic is set together with the answer, without names; no person reads along.
7. A question with no answer goes as a topic, without a name and without the asker's words, to the subject's owner. A topic asked once goes in only when it comes a second time; after three months it goes only into the sum across all teams.
8. A wrong answer is a finding about Inora and the source, never about the member of staff who came across it.
9. 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 is our competence register for reserved and high-risk procedures under our training policy: the assessor signs off the practical assessment, and from then on it stays current with the procedures the member of staff reports doing themselves, with the protocol and the version that applied. The care worker's questions to Inora never count, not even as evidence of competence. It records the procedure, the protocol with its version, the date, on whose instruction and who signed off the practical assessment, never the content of a conversation, a score or a usage figure. In the pilot the record is a preview for the participating team and staff take part voluntarily; it becomes our official register only after your consent. It stays in Inora for as long as the member of staff works for us, plus 30 days; in those 30 days we export it to our own personnel file. Only our team lead and training department see the competence record, and the member of staff themselves. The member of staff sees their own competence record in Inora and receives a copy on request. The record log shows, once Inora reads the record, through a connection or the user's own login, per step what Inora did and on whose behalf. The function the organisation appoints sees it only on written request, per client or in an investigation, to check record access; it is no figure about a member of staff and never holds what anyone asks.
10. The time Inora gives back goes to care. A decision on staffing is a decision of its own, which we put to you separately.

11. We switch on the test set only if you consent to it separately below. No person reads a question or answer in the test set; testing a new version is automated. If you withdraw the consent for the test set, Axiomatic deletes the test set within 30 days.

Conditions 1 to 9 and 11 also stand in the data processing agreement with Axiomatic, Axiomatic's privacy statement (Staff conversations) and the page Inora and the EU AI Act (What Inora never does). Condition 10 is an agreement within our organisation and stands in this decision only. Axiomatic weakens no condition without our written consent.

Article 5. Evaluation. We evaluate the introduction with you after the eight-week pilot and every year after. For that you receive the monthly report per team and an overview of every access by Axiomatic (article 4, condition 5), without its content.

Article 6. Change. If we want to change these conditions, or deploy Inora for another purpose, we put that to you as a new request for consent. If we use Inora other than on these conditions, that is a decision without your consent. You can then invoke its nullity in writing, within one month of our telling you of that use or of it becoming apparent to you (WOR article 27(5)), and we stop that use.

Article 7. Our request. We ask you to consent to this decision, on the conditions in article 4. We would welcome discussing it with you at the consultation meeting of [date of the meeting], before the rollout to more teams after the pilot. After your decision we let you know in writing which decision we take and the date it takes effect.

Kind regards,

[Name], for the board of [name of the organisation]

Signature: _____

Decision of the works council

To be filled in by the works council.

Field	Entry
Discussed at the consultation meeting of	
Decision on the request	Consent / no consent
Test set (condition 11)	Consent / no consent
Reasons	

Field	Entry
Date and signature of the chair	

AXIOMATIC

Quality and clinical pack

Inora, for quality, the nursing council and the care director

This pack follows the document on Inora and the AI Act, and the supplier file. Where they differ, the articles of the signed agreement prevail.

Version 1.8, 9 November 2026

1. What this pack settles

This pack is for the quality adviser or manager, the nursing advisory council, the care director or elderly-care physician and the head of education of a care organisation that is evaluating Inora. It answers one question: does every answer come from our own protocol? Yes, every answer comes from your own protocol.

The answer in one paragraph. Inora answers from your own organisation's agreements and shows, for every sentence, the source, the version and the passage. If the answer is not in your sources, Inora says so, and where it looked. The professional decides; that intended use is fixed word for word and keeps Inora outside the medical device rules. A document counts in Inora only once it has passed your own route. For every answer Axiomatic records what it rested on, without who asked. When something fails, we investigate the system, never the professional.

2. The intended use

What a system may do follows from its intended use. For Inora it reads, word for word:

> Inora supports professionals with their organisation's knowledge. It answers questions from your sources and shows each of your organisation's sources with one tap, puts what a professional wrote into your report formats and shows what your protocols still ask for. It prepares the follow-up that results, such as the request to the doctor, the list in the record or the check; it goes out only with the professional's approval, and the professional decides.

Inora does not diagnose or decide on treatment (Art. 4.2). Besides: the professional decides and is responsible for the decision; an answer from Inora does not replace the professional's judgement (Art. 4.3).

2.1 Triage

Inora supports triage. The nurse triages, scores and decides. Inora puts the organisation's own protocol beside the nurse, and flags what is missing.

Step	The nurse	Inora
Assess	Sees the client, asks and measures.	Puts your organisation's triage protocol beside the nurse, question by question.
What is missing	Fills in what they don't know yet.	Flags what the protocol still asks for, such as a respiratory rate not yet recorded.
Urgency	Decides how urgent it is.	Never.
Decision	Decides: act themselves, call the doctor or the back-up.	Never.
Record	Reads and signs the report.	Readies it, with the protocol and the version in force; on the nurse's approval it goes into the record.

Inora readies the report; the nurse reads and signs, and only on that approval does Inora file it in the client record; Inora acts on that person's behalf, never with more rights than they have.

2.2 What Inora never does

- It does not diagnose, give a prognosis or decide on treatment.
- It does not assess photos of skin or wounds.
- It does not triage in the nurse's place.
- It does not evaluate staff or take decisions about their work.
- It does not decide whether anyone is eligible for a service.
- It infers no emotion or mood of staff, from voice or face.

3. Where Inora stands in law

Rule	What it says	What it means for Inora
Regulation (EU) 2017/745 (MDR), Art. 2, point 1	Software is a medical device when its manufacturer intends it for a specific medical purpose, such as diagnosis, prediction or treatment.	Inora is not intended for that. Its intended use keeps it outside the medical device rules.
Regulation (EU) 2024/1689 (AI Act), Art. 5(1)(f)	No emotion recognition in the workplace, since 2 February 2025.	Inora infers no emotion or mood.
AI Act, Art. 4	AI literacy, since 2 February 2025, amended as of 27 July 2026 (Regulation (EU) 2026/1744): providers and deployers take measures to support the AI literacy of their staff and of others who work with the system on their behalf. They need not guarantee any specific level for any individual.	We support the AI literacy of whoever works with Inora: what it does, what it never does and how to check a source. We give the training at implementation; your organisation receives the material for its own measures.
AI Act, Art. 50(4)	Published AI text is disclosed, since 2 August 2026.	If an organisation does publish AI text to inform the public on a matter of public interest, it discloses that the text is AI-generated, unless a person has reviewed it and the organisation or a member of staff holds editorial responsibility.
AI Act, Art. 25(1)(c)	Whoever puts a system to a use outside its intended use can become the provider of a high-risk system.	Use Inora within the intended use of section 2.

Inora is not a high-risk AI system: the care professional assesses and decides, and Inora supports them with the organisation's own protocols. With every answer the member of staff sees that Inora drafted it, with its source (transparency, Article 50), and your organisation keeps a record of who was trained to work with Inora (AI literacy, Article 4).

Roles under the AI Act: Axiomatic B.V. is the provider; your organisation is the deployer; the providers of the general-purpose models carry the duties for their models (Art. 53).

Sources: MDR, AI Act, Regulation (EU) 2026/1744.

4. Who answers for what

- **The care provider** answers for good care and for the means it uses for it (Care Quality, Complaints and Disputes Act, Art. 2 and 3). That stays so with Inora.
- **The professional** decides and is responsible for the decision.
- **Axiomatic** answers for what Inora does with your sources; your organisation answers for what your sources say.

5. How an answer is made, and when Inora refuses

Every sentence of an answer rests on a source of your organisation and ends in a mark. One tap on the mark shows the title, the version and the passage the answer comes from. If the answer is not in the sources, Inora says so, shows where it looked and gives no answer from general knowledge. The question goes as a topic, without a name and without the asker's words, to whoever owns the subject.

An example, as the quality page shows it:

	Answered	Not in the sources
Question, 03:12 and 03:40	'I'm alone on the ward tonight and have to give morphine. Who does the double check?'	'She wants to take her own CBD oil alongside the morphine. Is that allowed?'
Inora	The on-call nurse, by video call in the medication administration system. If the nurse doesn't answer within 15 minutes, call the back-up and record that the check was done by phone.	That isn't in your sources, so I won't answer it. What they do say: an over-the-counter remedy alongside prescribed medication only after consulting the pharmacist.
What it rests on	Medication policy MED-04, 4.3, version 7 (adopted 12 June 2026, owner medication committee); Night on-call agreement ORG-12, 2, version 3.	Searched the medication policy (5, Over-the-counter remedies), the formulary 2026 and the pharmacy agreement: no passage. As a topic, without a name, without the asker's words and without the client, to the medication committee.

84% of questions on the inspectorate's risk themes (medication, restraint, wounds, falls and infection) call for the organisation's own protocol. That is why an answer rests on your protocol, not on general knowledge.

6. How a document enters Inora

A document enters Inora the way it enters your handbook.

Role	What it does
The owner	Every document has one at your organisation: a committee, a team or a role. A question without an answer reaches the owner as a topic, without the name or the words of who asked.
Author and content experts	Write and review as in your own document control. Inora changes not a word.
Whoever adopts it	The quality adviser publishes, or the nursing council, as your route prescribes. Only then does a document count in Inora.
Drafts and old versions	Do not count. A replaced version is kept, so you can check what applied on any day.

The life of one document:

Date	Who	What
9 March 2026	A question without an answer	Topic: double check at night, alone on the ward · 2×. Version 6 did not say. Forwarded to the medication committee, without a name and without the care worker’s words.
12 May 2026	Elderly-care physician, author	Writes section 4.3 for version 7.
26 May 2026	Pharmacist and two nurses	Review it as content experts.
12 June 2026	Quality adviser, on the nursing council’s advice	Adopts and publishes it. From that day Inora answers from version 7; version 6 no longer counts.
2 November 2026	An answer to the same question	Rests on 4.3, version 7.

7. Before day one: the intake of your handbook

Every implementation starts with the quality handbook, together with your quality adviser: who owns each document, which version applies and what has expired. You receive the outcome document by document, with the reason. In one quality handbook of 350 documents, 17 subjects were filed more than once, and for 8 of them the versions say different things. Besides that, 21 documents were past their own review date, and some files were stored as images no search can read (export of 24 September 2026, counted by file hash, text comparison and the handbook's own header fields).

What happens to a finding:

What the intake finds	What happens to it
Two versions of one subject	The owner chooses which counts; the other goes.
Review date passed	To the owner, asking whether it still applies.
Stored as an image	Turned into text; the owner approves it before it counts.
A password or personal data in a document	To the owner, never into an answer.

For every source that is not your organisation's own, the licence list states the ground on which Inora uses it.

8. What is on record, and for whom

For every answer Axiomatic 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 and the ward are not in it, and the record stays with Axiomatic. On written request, for an incident or a complaint, you receive it.

You request it by date and source, or by that reference, which the nurse can put in their report or incident report themselves. If you ask within the conversation's retention term (90 days by default), we also look up the conversation by the same route and hold it until the investigation closes; after that, only the record remains, which is kept for 2 years. The member of staff is told that their conversation was read.

Field	What it holds
Date	The date of the answer, not the time.

Field	What it holds
Sources	Each document with section, version and adoption date.
Model	The language model the system picked, in the EU, with its version.
Test set	The version of your test set this version of Inora passed.
Reference	The reference the nurse sees with the answer; it does not say who asked.
Not in it	Who asked, the time, the ward, the question and the answer.

The record stays with Axiomatic in Europe (Ireland) and is deleted automatically after that term, from back-ups too within 30 days.

With your organisation: what a worker sends themselves, such as their report or their incident report; topics without an answer, per owner; use per team of at least five people, never per person; the competence record the inspectorate expects (Wkkgz, Wet BIG), as a record of its own with a name, apart from every answer.

Never with your organisation: who asked what; a worker's conversation; a figure or score per person; how often one worker looks something up; a competence derived from a question or an answer. The answer record stays with Axiomatic; you receive it on written request. Axiomatic reads a conversation only on a written request from the function you name for it, 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. 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.

8.1 The competence record

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 sits in Inora Matrix, your competence register for reserved and high-risk procedures under your training policy: the assessor signs off the practical assessment, and from then on it stays current with the procedures the member of staff reports doing themselves, with the protocol and the version that applied. The care worker's questions to Inora never count, not even as evidence of competence. In the pilot it is a preview for the participating team, until the works council consents. It is your own record; Axiomatic keeps it in Inora as processor, on your instruction. It is a record of its own with the worker's name, apart from every answer: Inora never makes it from a question or from the

record of an answer. 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. The competence itself you assess, as your training policy prescribes.

Field	Example
Care worker	Sanne de Wit, senior care assistant
Procedure	Subcutaneous insulin injection, a reserved procedure
Protocol	Insulin administration, version 6
Date	14 October 2026
On whose instruction	The client's attending physician

It stays in Inora for as long as the care worker works for you, plus 30 days; in those 30 days you export it to your own personnel file, where your own term applies. Only your team lead and training department see the competence record, and the member of staff themselves. The member of staff sees their own competence record in Inora at any time and receives a copy on request: that is their right of access (article 15 GDPR), which you answer and Axiomatic helps with. Article 5.6 of the data processing agreement„ binds it.

9. The system is at the centre of every investigation

A failure in an answer comes from the system: from a source that is out of date, from a version of the model, from the software around it, from a setting or from our own way of working. That is where we look for the cause, never at the professional who came across the failure. Five steps, every time:

1. **Tell.** We tell whoever the failure affects first; a breach no later than 24 hours after becoming aware.
2. **Restore.** The work goes back to a version that works, the previous one where needed.
3. **Investigate.** Without blame: in the source, the model, the software around it, the configuration and our own way of working. No finding names whoever came across the failure.
4. **Write it down.** What we find, your organisation receives in writing. If the investigation is still running, we add to it.
5. **Change.** The change goes into the system, with a test that keeps the same failure from getting through unnoticed again.

After a calamity Axiomatic delivers a first finding within 5 working days and a report within 4 weeks, inside the eight weeks the inspectorate gives you for your own investigation (Uitvoeringsbesluit Wkkgz, art. 8.7(2)), after your report (Wkkgz, art. 11).

9.1 Your test set, before every new version

We test every new version on your organisation's own questions before your staff work with it: real questions, stripped of the names of clients and staff, only on your written instruction, after the works council's consent where you have one; no person reads them. Every past failure goes into it as a test that stays. If a version does worse than the one before on a single question, it is held back, fixed and tested again.

9.2 Available, day and night

At night too. Your sources stay in your own document system; Inora works with a copy that your handbook manager supplies and keeps up to date. Inora is built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night.

10. What your organisation does

- Use Inora within the intended use of section 2.
- Name your sources and keep them current. Every document has an owner at your organisation.
- Take measures to support your staff's AI literacy (AI Act, Art. 4, as amended from 27 July 2026). We give the training at implementation.
- Let the professional decide.
- Involve your works council (Works Councils Act, Art. 27(1)(k) and (l)).
- Disclose AI text you publish.
- Report what goes wrong.

11. What you receive from us

Document	When
The intended use, word for word	Before the first question
This quality and clinical pack	Before the first question
The outcome of your handbook intake, document by document with the reason	Before day one
The licence list	Before day one
The AI literacy training material	At implementation
The report of a failure, with the finding and the test	At every incident

Contact: support@axiomatic.digital. Axiomatic B.V., Delft, Chamber of Commerce number 97816825.

12. Inora and the AI Act, in full

This document describes Inora for the AI Act, Regulation (EU) 2024/1689: for the organisations that deploy Inora, their data protection officer, their works council and anyone who supervises them.

About this document

- **System:** Inora
- **Provider:** Axiomatic B.V., Delft, Chamber of Commerce number 97816825
- **Contact:** support@axiomatic.digital

We update this document when Inora, the models it uses or the rules change, and after a serious incident.

Who has which role

- **Provider.** Axiomatic develops Inora and places it on the market under its own name. Under the AI Act we carry the provider's duties.

- **Deployer.** Each organisation that uses Inora under its own authority is a deployer. Its staff work with it.
- **Model providers.** Inora uses general-purpose AI models from other providers. Those providers carry the duties for their models, as Article 53 sets them out.

Inora is not a high-risk AI system: the care professional assesses and decides, and Inora supports with the organisation's own protocols. Inora's intended use falls in no category of Annex III. Annex III, point 5(d), names emergency healthcare patient triage systems; Inora does not triage and sets no priority. The nurse does, and Inora holds the organisation's protocol up beside them.

The duties that do apply, Inora meets: with every answer the member of staff sees that Inora drafted it, with its source (transparency, Article 50), and the organisation keeps a record of who was trained to work with Inora (AI literacy, Article 4).

The intended use

What a system may do follows from its intended use. For Inora it reads, word for word:

> Inora supports professionals with their organisation's knowledge. It answers questions from your sources and shows each of your organisation's sources with one tap, puts what a professional wrote into your report formats and shows what your protocols still ask for. It prepares the follow-up that results, such as the request to the doctor, the list in the record or the check; it goes out only with the professional's approval, and the professional decides.

Inora does not diagnose or decide on treatment. Its intended use keeps Inora outside the scope of the medical device rules.

What Inora never does

- It does not diagnose, give a prognosis or decide on treatment.
- It does not assess photos of skin or wounds.
- It does not triage patients. The nurse triages; Inora supports them with the organisation's own protocol and flags what is missing.

- It does not evaluate staff or take decisions about their work. Figures on use cover only teams of at least five people, never one member of staff, and no one gets a score. The competence record covers only reserved and high-risk procedures under the organisation's training policy; it is the organisation's own, records 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 their questions to Inora never count. The member of staff sees their own competence record in Inora and receives a copy on request (Article 15 GDPR); what that means for the works council is on Works council.
- It does not decide whether anyone is eligible for a service.
- It infers no emotions or mood of staff, from voice or face. Article 5(1)(f) prohibits that.

Whoever puts an AI system to a use outside its intended use can thereby become the provider of a high-risk AI system (Article 25(1)(c)).

Duties that apply now

- **AI literacy** (Article 4, since 2 February 2025, amended from 27 July 2026 by Regulation (EU) 2026/1744). Providers and deployers take measures to support the AI literacy of the people who work with the system on their behalf; they need not guarantee any level for any individual. Whoever works with Inora learns what it does, what it never does and how to check a source. We give the training at implementation, and the organisation receives the material for its own measures. Since the same date emotion recognition at work is prohibited (Article 5(1)(f)); how Inora keeps to that is under What Inora never does.
- **AI text an organisation publishes** (Article 50(4), since 2 August 2026). If an organisation does publish AI text to inform the public on a matter of public interest, it discloses that the text is AI-generated, unless a person has reviewed it and the organisation or a member of staff holds editorial responsibility.

The professional keeps oversight

The professional decides. Inora is built so that they can see what an answer rests on, and contradict it:

- Each of the organisation's sources is marked in the answer. One tap on the mark shows the title, the version and the passage the answer comes from.
- If the answer is not in the sources, Inora says so, and where it looked. The topic goes, without the asker's name or words, to the owner of the source, so the source can be completed.

- In a report, the professional's own words go under the organisation's headings. Inora readies the report; the professional reads and signs, and on that approval Inora files it in the client record; Inora acts on that person's behalf, never with more rights than they have.
- Inora acts only once a person approves.

Where it runs

Inora runs in the EU or on an organisation's own servers. The system picks the language model for each task; who provides it is on Sub-processors. Every new version is tested before staff work with it; on the organisation's written instruction, on its own test set too.

For the team reports the language model that writes the answer sorts the conversation by topic in the same step, in the EU, or on an organisation's own servers inside its network. No person reads along, and the model keeps nothing. The sorting stays in the environment and is deleted with the conversation.

No one trains or fine-tunes a model on an organisation's documents, questions, answers or reports: not us, and not any model provider.

Data	From whom	What for
Sources: documents, protocols, work agreements	The organisation	The answers
Conversations: questions, answers and reports, and the topic of each conversation, without names	The organisation's staff	The conversation itself, and the topic for the team reports, sorted in the same step as the answer; kept 90 days by default. If the organisation asks Axiomatic, within the retention term, to read a conversation for an incident or a complaint, Axiomatic holds it until the investigation is complete and deletes it within 30 days after; the member of staff is told
Answer record: per answer the sources with their versions, the check and the date, and a reference the member of staff sees with the answer; never who asked, the time, the ward, the question or the answer	Axiomatic, of every answer	Accounting for what an answer rested on, for an incident or a complaint; 2 years, at Axiomatic

Data	From whom	What for
Test set: questions from the organisation and flagged answers with their question, stripped of the names of clients and staff	The organisation, only on its written instruction, after the works council's consent where it has one	Testing every new version before it goes live; no person reads a question or answer for it; kept until it withdraws the instruction, at the latest until the end of the agreement, then deleted within 30 days

What we process and why is in the privacy statement.

For organisations that deploy Inora

- **Use Inora within its intended use.** Use it to support triage, never to triage in the professional's place; do not use it to evaluate staff or decide eligibility for services, and do not let it assess photos of skin or wounds.
- **Designate your sources and keep them current.** What Inora says about your organisation rests on the sources you designate. Each document has an owner in your organisation. An outdated protocol gives an outdated answer.
- **Support your staff's AI literacy** (Article 4, as amended by Regulation (EU) 2026/1744). Whoever works with Inora learns what it does, what it never does and how to check a source. We give the training at implementation.
- **Let the professional decide.** Inora supports; the professional takes the decision.
- **Involve your works council.** The works council has a right of consent over a system that processes staff's personal data or can monitor their behaviour or performance (Article 27(1)(k) and (l) of the Dutch Works Councils Act).
- **Disclose AI text you publish,** as set out above under Article 50(4).
- **Report what goes wrong.** If Inora answers wrongly, goes past the line of its intended use, or refuses a question your sources answer, report it to your quality team and to us.

13. The licence list

For every source that is not your organisation's own, it states the basis on which Inora uses it. Inora rests an answer on a national reference only where its publisher allows it. The care worker does not see it: no marker and no link. The record of the answer keeps it. The attribution an open licence asks for appears on a fixed page in Inora's legal notice.

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.

AXIOMATIC

Responsible disclosure

If you find a weakness in Inora, on axiomatic.digital or in the infrastructure we operate, report it to us. We confirm every report and keep you informed until it is closed.

Updated on 9 November 2026

Why this matters

Care organisations put their protocols, work agreements and quality handbook into Inora. Their staff type questions and reports into it that can concern clients, and so can contain health data. A weakness in Inora therefore affects not only us, but care organisations, their staff and their clients. We would rather hear about it from you than from someone who abuses it.

How we protect Inora and that data is on the Security page.

What this policy covers

- Inora's web application, in which the staff of care organisations ask questions and write reports.
- Inora's APIs.
- This website, axiomatic.digital.
- The infrastructure Axiomatic itself operates for Inora and for this website.

What it does not cover

- Services and integrations run by others, such as a care organisation's identity provider (for example Microsoft Entra ID) or its electronic client record. Report a vulnerability there to that organisation or to its maker. If it also affects Inora, tell us as well.
- Social engineering and phishing of Axiomatic's staff or of care organisations' staff.
- Attacks that overload or take down the service (DoS and DDoS).
- Automated scanning or testing that makes the service slower or unavailable for others.

- Physical attacks on offices or data centres.
- Software and systems that are not Axiomatic's.

How to report

Email security@axiomatic.digital with "Security" in the subject line.

In your report, include:

- what the vulnerability is and what someone could do with it;
- the steps to reproduce it;
- what shows it, such as screenshots, a proof of concept or requests and responses;
- how we can reach you with questions.

Do not send us other people's data you came across. Describe what you saw, not the data itself.

The address and this policy are also in security.txt on axiomatic.digital, following RFC 9116.

What we do, and when

- **Receipt.** We confirm receipt of your report within three working days.
- **Assessment.** We investigate the report, set its severity by the classes below and tell you what we find.
- **Fix.** We fix a critical vulnerability within 72 hours and others within 30 days. If we cannot, we tell you why and when we will.
- **Keeping you informed.** Until the vulnerability is fixed, we keep you informed of our progress.
- **Care organisations.** If the vulnerability let a care organisation's data be viewed, changed or lost, we notify that organisation without undue delay, no later than 24 hours after we become aware of it, as the Security page describes.
- **Credit.** With your permission, we credit you once the vulnerability is fixed.

What we ask of you

- Do not access, change or delete data that is not yours.
- If you come across data of a care organisation, a member of staff or a client, stop at once, tell us and keep no copy.
- Do not disrupt the service. It is used at night too, when there is no colleague to fall back on.
- Test only with accounts you own or have explicit permission to use. Inora has no public sign-up: every account is created by a care organisation, through its own sign-in. If you want to test Inora yourself, ask us for access.
- Use a vulnerability no further than needed to show it.
- Publish nothing before the vulnerability is fixed, and give us 90 days from your report for that. If it is fixed sooner, we agree together when you publish.
- Do nothing beyond what this policy allows.

What we commit to

If you follow this policy and act in good faith, we will not report you to the police or take legal action against you. If someone else holds you to account, we will state that you acted within this policy. We cannot waive action on behalf of others, such as the Public Prosecution Service or a care organisation.

We treat your report and your details as confidential, and share your name only with your permission.

How we set severity

Class	Examples
Critical	Remote code execution; bypassing sign-in; access to another organisation's environment; viewing conversations, reports or documents at scale; obtaining keys or secrets.
High	Gaining more rights within an organisation than one's own account gives; viewing another member of staff's conversations; stored cross-site scripting; SQL or command injection; making Inora answer outside the organisation's sources or judge a client.

Class	Examples
Medium	Cross-site request forgery; leaking data without sensitive content; access-control faults with limited impact.
Low	Verbose error messages, missing security headers and other departures from good practice with little impact.

We look at what an attacker can achieve in practice, not only at the type of fault. Where client data is involved, we weigh the report more heavily.