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.