AXIOMATIC

Leveranciersdossier

Elk stuk van Axiomatic B.V. over Inora, met voor wie het is en wanneer het komt.

7 november 2026

Inhoud

ICT-dossier	pagina 5
Beveiligingsoverzicht	pagina 14
Controlematrix	pagina 25
Subverwerkers	pagina 39
Privacydossier	pagina 43
Dossier voor de ondernemingsraad	pagina 53
Informatiebrief en model voor het instemmingsverzoek	pagina 66
Kwaliteitsdossier	pagina 76
Privacyverklaring	pagina 91
Een kwetsbaarheid melden	pagina 109

Alle stukken

Vóór de eerste vraag

Stuk	Voor	Waar
Subverwerkers Wie verder gegevens verwerkt, en waar.	FG, ICT	pagina 39

Stuk	Voor	Waar
Controlematrix Elke beheersmaatregel van NEN 7510 en ISO 27001, en hoe wij die hebben ingericht. Elk kwartaal bijgewerkt, elk jaar getoetst aan wat in productie draait. De basis voor uw verklaring van toepasselijkheid.	Bestuur, ICT	pagina 25
ICT-dossier Wat dag één uw team kost, waar de gegevens staan, wie erbij kan, en elke maatregel.	ICT	pagina 5
Privacydossier met de DPIA voorgevuld De DPIA voorgevuld: de rollen, en elke verwerking met doel, plaats en termijn.	FG	pagina 43
OR-dossier Wat de organisatie krijgt en wat nooit, het teamverslag, en elke regel met zijn clausule.	OR	pagina 53
Kwaliteitsdossier Uw protocollen bepalen elk antwoord, elk document heeft een eigenaar en bij fouten staat het systeem centraal.	VAR, Kwaliteit	pagina 76
Beveiligingsoverzicht (volledig) Elke beveiligings-maatregel, en de koppeling met uw identiteitsbeheer.	Bestuur, ICT	pagina 14
Beveiliging Inora en uw gegevens zijn beveiligd, met vaste maatregelen voor bescherming en herstel.	ICT	Online op axiomatic.digital
Privacyverklaring Wat wij verwerken, waarom, waar en hoe lang.	FG, OR	pagina 91
Gebruiksaanwijzing Wat Inora doet en nooit doet, hoe u het inzet, en wie bij u toezicht houdt op het gebruik.	VAR, Kwaliteit	Op verzoek, zonder voorwaarde
Continuïteit Uw kennis als u stopt, als wij stoppen of als Axiomatic van eigenaar wisselt.	Bestuur, RvT, FG, Inkoop	Online op axiomatic.digital
Een kwetsbaarheid melden Hoe u een kwetsbaarheid in Inora of op deze site meldt, en wat wij daarna doen.	ICT	pagina 109
Licentielijst Van elke bron die niet van uw organisatie is: op welke grond Inora haar gebruikt.	Kwaliteit	Op verzoek, zonder voorwaarde
Uitkomst van de intake van uw handboek Wat dubbel staat, elkaar tegenspreekt of verlopen is, per document met de reden.	Kwaliteit	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie

Stuk	Voor	Waar
Informatiebrief en model voor het instemmingsverzoek Wat Inora verwerkt en bewaart, wie wat ziet, en dat geen verslag een medewerker noemt.	OR	pagina 66
Eén pagina voor de verpleegkundige adviesraad Wat Inora doet en nooit doet. Een nieuwe richtlijn telt pas na de adviesraad of uw eigen documentroute: eigenaar, auteur, twee inhoudsdeskundigen, kwaliteitsadviseur.	VAR	Op verzoek, zonder voorwaarde
Notitie voor de cliëntenraad Wat er voor cliënten verandert als hun zorgteam met Inora werkt.	Cliëntenraad	Op verzoek, zonder voorwaarde
De vermelding voor uw AI-register Compleet: aanbieder, beoogd gebruik, welke gegevens waar en wie ervoor instaat.	Bestuur, Kwaliteit	Op verzoek, zonder voorwaarde
Eén pagina voor de raad van toezicht Wat Inora doet en waar het stopt, wie aanbieder en wie gebruiksverantwoordelijke is, en welke cijfers elk kwartaal meegaan.	RvT	Op verzoek, zonder voorwaarde

Bij de overeenkomst

Stuk	Voor	Waar
Het beoogde gebruik, woord voor woord Wat Inora doet en nooit doet, om letterlijk te citeren. Het houdt Inora buiten de MDR.	Bestuur, Kwaliteit	Online op axiomatic.digital

Elke maand

Stuk	Voor	Waar
Maandverslag per team Per team naar de teamleider en de OR, voor teams van minstens vijf, nooit per medewerker.	OR	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie
Maandverslag over alle teams Opgeteld over alle teams, voor bestuur en kwaliteit; geen verslag per team, geen naam.	Bestuur, Kwaliteit	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie

Elk kwartaal

Stuk	Voor	Waar
Cijfers over alle teams voor het kwartaalverslag Wat de bestuurder elk kwartaal meeneemt naar de RvT, naast audits en incidentanalyses.	Bestuur, RvT	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie

Bij elke nieuwe versie

Stuk	Voor	Waar
Wat er veranderde, bij elke nieuwe versie Wat elke nieuwe versie verandert, met de uitkomst van de toets: nieuwe functies melden wij vooraf, beveiligingsupdates achteraf.	ICT, Kwaliteit	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie

Bij een incident

Stuk	Voor	Waar
Melding en verslag van een datalek Onze melding binnen 24 uur, daarna ons verslag.	Bestuur, FG	Vertrouwelijk: alleen voor de lezer, met de gegevens van uw organisatie

Op verzoek

Stuk	Voor	Waar
Uitleg voor de training van uw bestuurders Voor de Cyberbeveiligingswet: wat Inora is, waar het stopt en hoe het beveiligd is.	Bestuur	Op verzoek, zonder voorwaarde

AXIOMATIC

ICT-dossier

Inora, voor de CISO en de ICT-manager

Versie 1.13, 11 november 2026

1. Wat dit dossier regelt

U bent CISO of ICT-manager van een zorgorganisatie, en een collega wil met Inora beginnen. Uw vraag: kost dit mijn team werk? Dit dossier beantwoordt die vraag zo volledig dat u in één gesprek ja kunt zeggen, en het is zo opgezet dat u het in uw eigen archief legt.

Inora is het kennissysteem van de organisatie: zorgmedewerkers krijgen antwoord uit de eigen protocollen en werkafspraken. Axiomatic bouwt Inora, voert het zelf in en beheert het. Inora is ingericht volgens NEN 7510 en ISO 27001.

In het kort:

- **Uw team doet niets om te starten.** Eén toestemming in uw identiteitsbeheer. Verder niets. Medewerkers loggen in met single sign-on; er is niets te installeren.
- **Uw gegevens verlaten de EU nooit.** Eén eigen omgeving per organisatie bij Amazon Web Services in Ierland, het taalmodel in EU-regio's, of alles op uw eigen servers.
- **Alleen de engineers die Inora bouwen, kunnen bij productie:** elk bij naam in de verwerkersovereenkomst. Persoonlijke accounts met MFA, elke toegang vastgelegd.
- **Elke maatregel staat op papier**, in de controlematrix in hoofdstuk 5.
- **Wat de Cyberbeveiligingswet van uw bestuur vraagt, ligt klaar**, per plicht met het document.

2. Waarom u gelijk hebt om het te vragen

- **Besluit elektronische gegevensverwerking door zorgaanbieders, artikel 3, lid 2.** De zorgaanbieder zorgt volgens NEN 7510 en NEN 7512 voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem. Bron: wetten.overheid.nl, BWBR0040238.
- **Inspectie Gezondheidszorg en Jeugd.** Wie zijn ICT uitbesteedt, blijft als zorgaanbieder zelf verantwoordelijk voor de informatiebeveiliging. Bron: igj.nl, Vragen over NEN 7510.

- **Cyberbeveiligingswet, sinds 15 augustus 2026.** Artikel 21, lid 3, onder d noemt de beveiliging van de toeleveringsketen als deel van de zorgplicht; artikel 24 legt de goedkeuring van de maatregelen en de kennis om ze te beoordelen bij het bestuur; artikel 26 vraagt een vroegtijdige waarschuwing binnen 24 uur. Bron: wetten.overheid.nl, BWBR0052872.

Een leverancier van AI is dus een risico dat u draagt. Dit dossier laat zien hoe klein Inora dat risico maakt, en waar het op papier staat.

3. Dag één: 0 uur ICT-werk, met single sign-on

Onderdeel	Wat uw team doet	Uren
Accounts	Niets. Medewerkers loggen in via uw eigen identiteitsbeheer, met SAML 2.0 of OpenID Connect; SCIM houdt de accounts bij. Met single sign-on bewaart Inora geen wachtwoorden; MFA en wachtwoordregels stelt u zelf in.	0
Netwerk	Niets te doen: geen VPN, geen firewallregel. De pilot vraagt geen koppeling; koppelingen komen daarna, en uw ICT zet ze aan. Dan geldt: Inora maakt de rapportage klaar; de zorgmedewerker leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft.	0
Installatie	Niets. Inora is een dienst in de browser en de app. Updates doen wij. Nieuwe functies melden wij een week vooraf, met de uitkomst van de toets; met uw schriftelijke opdracht, na instemming van de ondernemingsraad waar u er een heeft, toetsen wij ook op de vragen van uw eigen teams. Beveiliging-supdates gaan zonder week vooraf door, kritieke binnen 72 uur, na dezelfde toets; die melden wij achteraf.	0

De beheerder geeft Inora eenmalig toestemming in uw identiteitsbeheer en kiest welke groepen toegang krijgen; daarna houdt SCIM de accounts bij. Bij Entra ID, de meest gebruikte, geeft de toestemming in Entra ID geeft Inora alleen `openid`, `profile`, `email` en `User.Read`, gedelegeerd en alleen-lezen; uw groepen komen als claim in het inlogbewijs. Inora leest alleen de groepen die u aan de app toewijst, zodat de claim nooit overloopt. Geen toegang tot mail, bestanden, Teams of SharePoint.

Uw bronnen blijven in uw eigen documentsysteem staan; Inora werkt met een kopie die uw handboekbeheerder aanlevert en bijwerkt. U bepaalt daarna zelf welke groepen medewerkers toegang krijgen en wie documenten en instellingen beheert.

4. Waar het draait en wie erbij kan

4.1 Hosting en locatie

Onderdeel	Leverancier	Locatie
Toepassing, database, document-opslag, zoekindex	Amazon Web Services EMEA SARL, Luxemburg	Regio Europa (Ierland), eu-west-1
Back-ups	Amazon Web Services EMEA SARL	Regio Europa (Ierland), eu-west-1; verspreid over meerdere beschikbaarheidszones
Taalmodel en embeddingmodel	Amazon Bedrock, via het EU-inferentieprofiel	AWS-regio's in de EU

Op uw keuze draait Inora op uw eigen servers, binnen uw eigen netwerk; uw verwerkersovereenkomst noemt dan elke leverancier van die inrichting.

4.2 Het taalmodel

Het systeem kiest per taak een taalmodel dat in de EU draait: bij Amazon Web Services of bij Microsoft Azure in de EU-regio, met de aangepaste misbruikmonitoring van Microsoft. Beide staan op de lijst van subverwerkers. Op uw eigen servers draait het taalmodel binnen uw netwerk.

Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek.

Geen model traint op uw gegevens: niet bij Axiomatic, niet bij de leverancier van het model. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model. Azure OpenAI draait Axiomatic met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring). Elk model, en elke wijziging in Inora, wordt getoetst voordat uw medewerkers ermee werken; met uw schriftelijke opdracht ook op uw eigen vragen.

4.3 Eén omgeving per organisatie

Elke organisatie heeft een eigen omgeving: een eigen database, eigen documentopslag en een eigen zoekindex. Een vraag die binnen de ene organisatie wordt gesteld, kan alleen de documenten van die organisatie bereiken. De scheiding zit in de infrastructuur, niet alleen in de software.

4.4 Wie bij productie kan

- Alleen de engineers die Inora bouwen en beheren, elk bij naam in de verwerkersovereenkomst (bijlage 2). De adviseurs van Axiomatic, en ieder ander bij Axiomatic, hebben geen toegang tot de productieomgeving en niet tot gegevens van organisaties.

- Alleen persoonlijke accounts, met multifactorauthenticatie. Geen gedeelde accounts.
- Elke toegang tot de omgeving van een organisatie wordt vastgelegd (4.7).
- Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend, en iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).
- Werklaptops hebben volledige schijfversleuteling en automatische beveiligingsupdates. Vertrekt iemand, dan vervalt de toegang dezelfde dag.

4.5 Inloggen en sessies

Inloggen loopt standaard via de single sign-on van uw eigen identiteitsbeheer, met elke identiteitsprovider: Entra ID, Okta, Google of elke andere via SAML of OpenID Connect. De beheerder stelt dit zelf in één stap in; SCIM maakt accounts aan en sluit ze af. Schakelt u daar een account uit, dan kan die persoon niet meer inloggen; een open sessie eindigt uiterlijk acht uur nadat zij begon.

Met single sign-on bewaart Inora geen wachtwoorden. Die accounts schakelt uw beheerder in Inora uit.

4.6 Versleuteling

- Tijdens transport: TLS 1.2 of hoger, voor al het verkeer van en naar Inora en tussen de onderdelen.
- Bij opslag: AES-256 voor databases, documentopslag, zoekindexen en back-ups. De sleutels staan in AWS Key Management Service, in de EU; elk gebruik wordt vastgelegd.
- Tijdens het beantwoorden van een vraag zijn de vraag en de passages alleen ontsleuteld zolang het antwoord wordt gemaakt; het model bewaart ze niet.

4.7 Back-ups, logging en updates

- Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland), verspreid over meerdere beschikbaarheidszones; hooguit 24 uur aan gegevens gaat verloren. Elk kwartaal zetten wij een back-up terug als test.
- Een herstel uit back-up duurt ten hoogste 8 uur.
- Beveiligingsupdates voor kritieke kwetsbaarheden binnen 72 uur, andere binnen 30 dagen.

Zonder koppeling leest Inora het dossier in een eigen microVM per gebruiker, met de login en rechten van die persoon: de zorgmedewerker logt zelf in, Inora bewaart geen wachtwoorden en houdt de sessie alleen vast zolang de taak loopt; werk op schema loopt op een sessie die de naamdrager vooraf goedkeurde. Alleen in de systemen die de organisatie aanwijst.

Inora legt inlogmomenten, beheerhandelingen en elke toegang door medewerkers van Axiomatic vast, 12 maanden lang. Zodra Inora het dossier leest, via een koppeling of de eigen login, houdt Inora ook een dossierlogboek bij, ingericht volgens NEN 7513: per stap wat Inora deed en namens wie, in te zien door de functie die de organisatie aanwijst. Op verzoek krijgt een organisatie de beveiligingslogging van haar omgeving, opgeteld per team van minstens vijf mensen en per dag, en elke toegang door Axiomatic; een

dag met minder dan vijf inlogs staat er als ‘<5’. Inlogmomenten en IP-adressen van één medewerker gaan nooit naar de organisatie. Bij een beveiligingsincident onderzoekt Axiomatic het logboek zelf en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen.

4.8 Beschikbaarheid

Ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht. Een storing meldt u aan support@axiomatic.digital, dag en nacht. Bij een storing krijgt de contactpersoon van uw organisatie bericht per e-mail, tot de storing is verholpen.

4.9 Wat de EU nooit verlaat

Uw gegevens, de back-ups en de logging. Voor een organisatie in de EU draait Inora in de EU en verwerkt het taalmodel gegevens alleen binnen de EU.

5. Elke maatregel, en hoe die is ingevuld

De controlematrix: alle beheersmaatregelen uit ISO 27001 en de maatregelen die NEN 7510 voor de zorg toevoegt, elk met hoe Inora die invult en met zijn status. De matrix is de basis voor uw verklaring van toepasselijkheid.

Elke maatregel, met hoe die is ingericht, staat in de Controlematrix in dit dossier.

6. Per laag: wie het controleerde

6.1 Inora

Norm of toets	Wat het dekt	Door
Ingericht volgens NEN 7510 en ISO 27001	Elke maatregel en hoe die is ingevuld, in hoofdstuk 5	Axiomatic
Ingericht op 99,9% beschikbaarheid	Doel: 95% van de storingen binnen 4 uur opgelost; reactie binnen een uur, dag en nacht. Storingsbericht per e-mail aan uw contactpersoon.	Axiomatic
Penetratietest, elk jaar	De applicatie en de infrastructuur, op de OWASP Top 10 en de scheiding tussen organisaties; de samenvatting op verzoek	Een onafhankelijke specialist
Doorlopend scannen	Code, softwarebibliotheken, containers en de inrichting in de cloud, bij elke wijziging en elke dag	Axiomatic

Een kwetsbaarheid melden kan altijd: security@axiomatic.digital, met ‘Beveiliging’ in de onderwerpregel. Wij bevestigen de ontvangst binnen drie werkdagen.

6.2 De diensten van AWS en Microsoft eronder

De certificaten die Amazon Web Services en Microsoft publiceren voor de diensten waarop Inora draait, zoals AWS ze op 2 november 2026 op zijn eigen pagina's noemt, en Microsoft voor Azure op de zijne. Ze gaan over de diensten van AWS en Microsoft, niet over Axiomatic of Inora; Axiomatic draagt ze niet mee.

Dienst	Norm	Wat het dekt	Door	Bron
Hosting, Europa (Ierland)	ISO/IEC 27001:2022	Informatiebeveiliging	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Hosting	ISO/IEC 27017:2015	Beveiligingsmaatregelen voor clouddiensten	EY CertifyPoint	aws.amazon.com/compliance/iso-27017-faqs
Hosting	ISO/IEC 27018:2019	Persoonsgegevens in de cloud	EY CertifyPoint	aws.amazon.com/compliance/iso-27018-faqs
Hosting	ISO/IEC 27701:2019	Privacybeheer	EY CertifyPoint	aws.amazon.com/compliance/iso-27701-faqs
Hosting	BSI C5	Duitse cloudnorm; regio Ierland in de reikwijdte		aws.amazon.com/compliance/bsi-c5
Hosting	SOC 1, 2 en 3	Rapporten van de auditor, in AWS Artifact		aws.amazon.com/compliance/services-in-scope/SOC
Amazon Bedrock	ISO/IEC 27001, 27017, 27018, 27701	Bedrock in de reikwijdte, Bedrock Marketplace niet	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Amazon Bedrock	ISO/IEC 42001:2023	Beheer van AI-systemen	Schellman	aws.amazon.com/compliance/iso-42001-faqs
Amazon Bedrock	BSI C5	Bedrock in de reikwijdte		aws.amazon.com/compliance/services-in-scope/C5
Amazon Bedrock	SOC 1, 2 en 3	Bedrock in de reikwijdte		aws.amazon.com/compliance/services-in-scope/SOC
Microsoft Azure (Azure OpenAI)	ISO/IEC 27001, 27017 en 27018	Informatiebeveiliging, clouddiensten en persoonsgegevens in de cloud; welke Azure-diensten erin vallen, staat in de Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001

Dienst	Norm	Wat het dekt	Door	Bron
Microsoft Azure (Azure OpenAI)	SOC 2 Type 2	Het rapport van de auditor over Azure, elk half jaar, op te vragen in de Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

De fysieke beveiliging van de datacenters ligt bij Amazon Web Services. Het moederbedrijf van AWS is Amerikaans; wat dat betekent, staat in onze privacyverklaring.

7. De Cyberbeveiligingswet, plicht voor plicht

Plicht van uw bestuur	Artikel	Wat wij doen	Wat u in het dossier legt
Zorgplicht	21, lid 3, d: de toeleveringsketen	Elke maatregel staat beschreven, met hoe die is ingevuld. De verwerkersovereenkomst bindt ons eraan, en wij werken mee aan uw audit.	Beveiligingsoverzicht versie 1.4 en controlematrix versie 1.3, van 9 november 2026; verwerkersovereenkomst,
Meldplicht	26: waarschuwing binnen 24 uur	Een datalek of een vermoeden daarvan in uw omgeving melden wij uiterlijk 24 uur na kennisname, met wat u voor uw eigen melding nodig hebt. Het verslag volgt binnen tien werkdagen.	Melding en verslag van een datalek; Beveiliging
Training van bestuurders	24, lid 2 tot en met 5	Een uitleg voor uw bestuurders: wat Inora is, waar het stopt en hoe het beveiligd is.	Uitleg voor de training van uw bestuurders (op verzoek)
Eindverantwoordelijkheid	24, lid 1: het bestuur keurt goed	Eén partij staat ervoor in: wij bouwen Inora, voeren het in en beheren het, en blijven verantwoordelijk voor onze subverwerkers.	subverwerkers, versie 1.6 van 11 november 2026

8. Als er iets misgaat

- Wij melden een datalek of een vermoeden daarvan zonder onredelijke vertraging, uiterlijk 24 uur nadat wij ervan kennis hebben genomen. Dat is een maximumtermijn, geen wachttijd.
- Wij delen direct wat bekend is: de aard, de betrokken gegevens en mensen, de waarschijnlijke gevolgen en de maatregelen.
- Binnen tien werkdagen sturen wij een schriftelijk verslag: wat er gebeurde, wat de oorzaak was en wat wij veranderden.
- Uw termijn van 72 uur bij de Autoriteit Persoonsgegevens blijft van u en wacht niet op ons verslag. Uw 72 uur beginnen zodra wij u melden; onze 24 uur gaan eraan vooraf.

- Wij onderzoeken een fout zonder schuldvraag, met de oorzaak in het systeem.

9. Leveranciers, audits en het einde

- Wij staan in voor wat Inora met uw bronnen doet; u voor wat die bronnen zeggen.
- Wij blijven verantwoordelijk voor onze leveranciers. Een nieuwe subverwerker melden wij 30 dagen vooraf; u kunt bezwaar maken.
- Na afloop krijgt u alles kosteloos terug: documenten in hun eigen formaat, de rest machineleesbaar. Uit actieve systemen is alles uiterlijk op dag 30 weg, uit back-ups uiterlijk op dag 60, schriftelijk bevestigd.
- Wij werken mee aan audits door uw organisatie of uw auditor, over alle verplichtingen uit de verwerkersovereenkomst.

10. Wat u in het dossier krijgt

- Dit ICT-dossier.
- Het beveiligingsoverzicht, versie 1.4 van 9 november 2026, met elke maatregel.
- De controlematrix, versie 1.3 van 9 november 2026, de basis voor uw verklaring van toepasselijkheid.
- De lijst van subverwerkers, versie 1.6 van 11 november 2026.
- Op verzoek: de uitleg voor de training van uw bestuurders.

11. Contact

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

12. Zes regels die meeverhuizen met de server

Draait Inora bij ons of op uw servers: dit blijft gelden.

- **Geen model leert van uw gegevens.**
- **Elk antwoord met zijn bron en versie.** In elk antwoord is elke bron van uw organisatie gemarkeerd; één tik toont de titel en de versie waaruit het komt. Staat het antwoord niet in uw bronnen, dan zegt Inora dat, en waar het zocht.
- **Elke stap vastgelegd.** Inora legt bij elk antwoord elke stap vast: welke bronnen het las, in welke versie, en welke controle het antwoord doorstond. Op uw schriftelijk verzoek herleidt Axiomatic met dat logboek een fout antwoord tot zijn oorzaak in het systeem, nooit tot een persoon.
- **Ingericht volgens NEN 7510 en ISO 27001.**

- Een nieuwe subverwerker hoort u dertig dagen vooraf.
- Stopt u, dan krijgt u uw kennis kosteloos terug.

AXIOMATIC

Beveiligingsoverzicht

Axiomatic B.V. en Inora

Versie 1.4, 9 november 2026

1. Inleiding

Axiomatic B.V. ontwerpt, bouwt, implementeert en beheert Inora. Zorgmedewerkers stellen Inora een vraag in gewone taal en krijgen antwoord uit de bronnen die hun organisatie heeft aangewezen; één tik op een markering toont de bron van de organisatie waarop een zin rust. De eigen documenten van de organisatie zijn intern, en de vragen kunnen over cliënten gaan. Dit overzicht beschrijft hoe wij die gegevens beschermen: wie erbij kan, waar ze staan, hoe wij ze gescheiden houden, versleutelen, back-uppen en bewaken, en hoe wij herstellen.

Dit document is bedoeld voor de privacyfunctionaris, de informatiebeveiliger en de ICT-afdeling van een zorgorganisatie die Inora beoordeelt. Het hoort bij de beveiligingsmaatregelen waarnaar Bijlage 2 van onze verwerkersovereenkomst verwijst. De voorgestelde termijnen en maatregelen worden pas afspraken na bevestiging en ondertekening van de verwerkersovereenkomst.

2. Organisatie en mensen

2.1 Het team

De mensen die Inora bouwen, implementeren en beheren:

- Engineering bouwt en beheert Inora. De directeur is verantwoordelijk voor beveiliging en privacy binnen Axiomatic.
- Implementatie en partnerschappen werken met zorgorganisaties tijdens de implementatie, zonder toegang tot gegevens van organisaties of tot de productieomgeving.
- De adviseurs hebben geen toegang tot gegevens van organisaties of tot de productieomgeving.

Alleen met naam genoemde engineers hebben toegang tot de productieomgeving, vastgelegd in de verwerkersovereenkomst. Wij werken niet met externe krachten die toegang hebben tot de productieomgeving of tot gegevens van organisaties.

2.2 Geheimhouding en screening

Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend die ook na vertrek blijft gelden. Die verklaring is ook wat de Uitvoeringswet AVG vraagt van mensen die gezondheidsgegevens verwerken zonder eigen beroepsgeheim (artikel 30, lid 4 UAVG). Iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).

Iedereen leest en tekent onze beveiligingsregels bij de start en daarna elk jaar opnieuw.

2.3 Apparaten

Wij werken op laptops met volledige schijfversleuteling, automatische beveiligingsupdates, een firewall en een schermvergrendeling na enkele minuten. Gegevens van organisaties staan nooit op laptops. Een verloren of gestolen laptop melden wij dezelfde dag, en de toegang ervan trekken wij in.

2.4 Accounts en toegang

- Alleen persoonlijke accounts. Geen gedeelde accounts, geen gedeelde wachtwoorden.
- Multifactorauthenticatie op elk account dat toegang geeft tot code, infrastructuur, e-mail of documenten. Beheertoegang tot de productieomgeving vereist een fysieke beveiligingssleutel.
- Toegang tot de productieomgeving is beperkt tot de met naam genoemde engineers, en tot wat zij nodig hebben.
- Elke toegang door medewerkers van Axiomatic tot de omgeving van een organisatie wordt vastgelegd. Elk kwartaal controleren wij de toegangsrechten.
- Vertrekt iemand, dan vervalt zijn toegang dezelfde dag.

3. Opbouw

3.1 Eén omgeving per organisatie

Elke organisatie heeft in Inora een eigen omgeving: een eigen database, eigen documentopslag en een eigen zoekindex. Er is geen gedeelde database waarin organisaties alleen door een kolom van elkaar zijn gescheiden. Een vraag die binnen de ene organisatie wordt gesteld, kan alleen de documenten van die organisatie bereiken.

3.2 Inloggen

Inora koppelt aan de eigen single sign-on van de organisatie, meestal Microsoft Entra ID, via OpenID Connect of SAML 2.0. Met single sign-on bewaart Inora geen wachtwoorden; multifactorauthenticatie en wachtwoordregels stelt de organisatie in, in haar eigen identiteitsbeheer. Schakelt de organisatie daar een account uit, dan kan die persoon niet meer inloggen op Inora. Een al geopende sessie kan actief blijven tot deze wordt ingetrokken of verloopt. Een sessie eindigt uiterlijk na acht uur.

De toestemming in Entra ID geeft Inora alleen openid, profile, email en User.Read, gedelegeerd en alleen-lezen; de groepen van de organisatie komen als claim in het inlogbewijs. Geen toegang tot mail, bestanden, Teams of SharePoint. Inora leest alleen de groepen die de organisatie aan de app toewijst, zodat de claim nooit overloopt. Die accounts schakelt de beheerder van de organisatie in Inora uit.

Inora kent twee rollen. Beheerders beheren documenten, instellingen en het rapportageregister. Gebruikers stellen vragen en maken rapportages. De organisatie bepaalt welke groepen medewerkers welke rol krijgen.

3.3 Hoe een vraag wordt beantwoord

1. Een gebruiker stelt een vraag in Inora.
2. Inora zoekt in de eigen index van de organisatie naar de passages die over de vraag gaan.
3. De vraag en die passages gaan naar het taalmodel, binnen de Europese Unie.
4. Het model schrijft een antwoord op basis van de passages. Inora toont het antwoord met een markering bij elke zin die op een bron van de organisatie rust; één tik toont het document en de passage. Beantwoordt geen passage de vraag, dan zegt Inora dat, en waar het zocht.

5. De vraag, het antwoord en de bronnen worden bewaard in de gespreksgeschiedenis van de gebruiker, in de omgeving van de organisatie, voor de bewaartermijn die de organisatie heeft ingesteld.

Bij rapportages komen de kopjes uit een register dat de organisatie zelf bijhoudt. Het model schrijft alleen de inhoud eronder.

De bronnen van de organisatie blijven in haar eigen documentsysteem staan; Inora werkt met een kopie die haar handboekbeheerder aanlevert en bijwerkt. Er is geen koppeling met dat documentsysteem.

Het cliëntdossier blijft in het eigen ECD van de organisatie. Inora leest het met de login en rechten van de zorgmedewerker zelf, in een eigen microVM per gebruiker, dus de pilot vraagt geen koppeling. Koppelingen komen na de pilot, en de ICT van de organisatie zet ze aan.

Bij het opbouwen van de zoekindex gaan ook documentpassages naar het embeddingmodel in de EU. Voor het antwoord gaan de vraag en de gevonden passages naar het taalmodel; in dezelfde stap deelt het model het gesprek in naar onderwerp, voor de teamverslagen (hoofdstuk 6).

4. Hosting en locatie

Onderdeel	Leverancier	Locatie
Applicatie, database, documentopslag, zoekindex	Amazon Web Services (Amazon Web Services EMEA SARL)	Regio Europa (Ierland), eu-west-1
Back-ups	Amazon Web Services	Regio Europa (Ierland), eu-west-1
Taalmodel	Amazon Bedrock, EU-inferentieprofiel	Regio's van Amazon Web Services in de EU
Taalmodellen via Azure OpenAI; het systeem kiest het model	Microsoft Ireland Operations Limited (Azure OpenAI)	Een Azure-regio in de EU
Website axiomatic.digital (geen gegevens van organisaties)	Amazon S3 en Amazon CloudFront	Bestanden in regio Europa (Ierland); levering via het wereldwijde netwerk van CloudFront

Alle gegevens in Inora worden in de Europese Unie verwerkt en opgeslagen. Verwerking buiten de EU vereist eerst een schriftelijke wijziging van de afspraken met de organisatie. Voor doorgifte buiten de EER is bovendien een geldige grond uit hoofdstuk V AVG nodig; toestemming van de organisatie alleen volstaat niet. Toegang op afstand en ondersteuning vallen ook onder deze beoordeling. Artikel 3.5 van de verwerkersovereenkomst beschrijft dit.

De fysieke beveiliging van de datacenters is de verantwoordelijkheid van Amazon Web Services. AWS publiceert zijn eigen certificeringen en auditrapporten. Die gaan over de diensten van AWS, niet over Axiomatic.

De moederbedrijven, Amazon.com, Inc. en Microsoft Corporation, zijn Amerikaans; beide nemen deel aan het EU-VS-kader voor gegevensbescherming (EU-US Data Privacy Framework). Opslag in de EU sluit een verzoek van een buitenlandse overheid niet uit; hoofdstuk 13 beschrijft wat wij dan doen.

5. Versleuteling

- **Tijdens transport.** Al het verkeer van en naar Inora, en tussen de onderdelen ervan, gebruikt TLS 1.2 of hoger. Oudere protocollen worden geweigerd.
- **Bij opslag.** Databases, documentopslag, zoekindexen en back-ups zijn versleuteld met AES-256.
- **Sleutels.** De sleutels staan in AWS Key Management Service, in de EU; de toegang is beperkt en elk gebruik wordt vastgelegd.
- **Geheimen.** Wachtwoorden van diensten, API-sleutels en certificaten staan in een sleutelkluis, nooit in de broncode.

De grens. Tijdens het beantwoorden van een vraag zijn de vraag en de passages alleen ontsleuteld zolang het antwoord wordt gemaakt; het model bewaart ze niet. Dat gebeurt op onze servers en bij het taalmodel. Versleuteling tijdens transport en bij opslag voorkomt die verwerking van leesbare tekst niet. Dit is geen end-to-endversleuteling waarbij alleen de gebruiker de tekst kan lezen. Medewerkers met toegang tot de productieomgeving zouden de inhoud op dat moment in principe kunnen zien; hoofdstuk 2 beschrijft wie dat zijn en hoe hun toegang wordt vastgelegd.

6. Kunstmatige intelligentie

- **Model.** Inora gebruikt taalmodellen in Amazon Bedrock, via het EU-inferentieprofiel. Vragen en antwoorden worden alleen in regio's binnen de EU verwerkt. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model.
- **Azure OpenAI.** Het systeem kiest per taak het taalmodel; via Azure OpenAI draait het in een EU-regio. Axiomatic draait het met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).
- **Teamverslagen.** Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek.
- **Training en opslag.** Gegevens van organisaties worden niet gebruikt om modellen te trainen of bij te trainen, noch door Axiomatic, noch door de modelleverancier.
- **Zoekindex.** Om documenten doorzoekbaar te maken, zet Inora passages om in numerieke representaties met een embeddingmodel in dezelfde EU-inrichting. Die worden opgeslagen in de eigen index van de organisatie en verdwijnen met de documenten.
- **Bron op één tik.** Elke zin die op een bron van de organisatie rust, draagt een markering; één tik toont het document en de passage. Een taalmodel kan zich vergissen; met de bron kan de zorgmedewerker het controleren.
- **Grens.** Inora ondersteunt professionals met de kennis van hun organisatie. Het stelt geen diagnose, beslist niet over een behandeling en beoordeelt geen foto's van huid of wonden; bij triage triageren verpleegkundigen, en Inora legt het protocol van de organisatie naast hen en wijst aan wat ontbreekt. De professional beslist. Door dit beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.

7. Logging en bewaking

Inora legt inlogmomenten, beheerhandelingen en elke toegang door medewerkers van Axiomatic vast, 12 maanden lang. Op verzoek krijgt een organisatie de beveiligingslogging van haar omgeving, opgeteld per team van minstens vijf mensen en per dag, en elke toegang door Axiomatic; een dag met minder dan vijf inlogs staat er als '<5'. Inlogmomenten en IP-adressen van één medewerker gaan nooit naar de organisatie. Bij een beveiligingsincident onderzoekt Axiomatic het logboek zelf en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen.

- Inora legt ook wijzigingen in documenten en instellingen vast.
- Wij krijgen een melding bij herhaald mislukt inloggen, ongewoon verkeer, fouten en onbeschikbaarheid.
- De logging staat in de EU en kan niet door de applicatie worden gewijzigd.

8. Back-ups en herstel

- Wij maken dagelijks een back-up van de omgeving van elke organisatie; hooguit 24 uur aan gegevens gaat verloren. Een herstel uit back-up duurt ten hoogste 8 uur.
- Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland), verspreid over meerdere beschikbaarheidszones.
- Elk kwartaal zetten wij een back-up terug in een aparte omgeving om te controleren of die volledig is.
- Ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht. Een storing meldt de organisatie via support@axiomatic.digital, dag en nacht. Bij een storing krijgt de contactpersoon van de organisatie bericht per e-mail, tot de storing is verholpen.
- Elk van de met naam genoemde engineers kan de dienst alleen herstellen. De herstelprocedure staat op papier.

9. Ontwikkeling en wijzigingen

- Elke wijziging in Inora wordt door een tweede engineer beoordeeld voordat zij in productie gaat.
- Ontwikkelen en testen gebeurt in een aparte omgeving zonder gegevens van organisaties.
- Wij controleren de softwarebibliotheken waarop Inora draait op bekende kwetsbaarheden. Beveiligingsupdates voor kritieke kwetsbaarheden voeren wij binnen 72 uur door, andere beveiligingsupdates binnen 30 dagen.
- De OWASP Top 10 is onze checklist voor de risico's van webapplicaties.

10. Testen

- **Penetratietest.** Elk jaar test een onafhankelijke specialist Inora, de applicatie en de infrastructuur, op de OWASP Top 10 en op de scheiding tussen organisaties. Kritieke bevindingen lossen wij op binnen 72 uur, andere binnen 30 dagen. De samenvatting van de laatste test krijgt u op verzoek.
- **Doorlopend scannen.** Code, softwarebibliotheken, containers en de inrichting in de cloud worden bij elke wijziging en elke dag automatisch gescand.
- **Beveiligingsonderzoekers.** Iedereen kan een kwetsbaarheid bij ons melden, volgens het beleid hieronder.

Een kwetsbaarheid meldt u door te mailen naar security@axiomatic.digital met ‘Beveiliging’ in de onderwerpregel. Wij bevestigen de ontvangst binnen drie werkdagen. Wij vragen onderzoekers geen gegevens van anderen in te zien of te wijzigen, de dienst niet te verstoren en ons 90 dagen te geven voordat zij publiceren. Tegen onderzoek dat te goeder trouw en binnen deze regels is gedaan, ondernemen wij geen juridische stappen.

11. Incidentbeheer

Wij werken met een vastgelegde incidentprocedure:

1. **Ontdekken.** Meldingen uit de bewaking, van gebruikers, organisaties of onderzoekers.
2. **Indammen.** De oorzaak stoppen en de schade beperken.
3. **Beoordelen.** Vaststellen om welke organisaties, gegevens en mensen het gaat.
4. **Melden.** Wij melden een datalek of een vermoeden daarvan zonder onredelijke vertraging, uiterlijk 24 uur na kennisname. Dit is een contractuele maximumtermijn, geen wachttijd. Een datalek kan ook bestaan uit verlies van beschikbaarheid, vernietiging of ongeoorloofde verstrekking. Wij delen wat bekend is over de aard, betrokken gegevens en mensen, waarschijnlijke gevolgen en maatregelen. Meldingen noemen de soorten gegevens en het aantal betrokkenen, nooit gegevens uit Inora. Aanvullingen volgen zodra ze beschikbaar zijn.

5. **Ondersteunen.** De zorgorganisatie is verwerkingsverantwoordelijke. Zij moet een datalek zonder onredelijke vertraging en, waar mogelijk, binnen 72 uur nadat zij ervan kennis heeft genomen melden bij de Autoriteit Persoonsgegevens, tenzij een risico voor de rechten en vrijheden van mensen onwaarschijnlijk is. Bij een waarschijnlijk hoog risico informeert zij de betrokkenen zonder onredelijke vertraging, tenzij een uitzondering uit artikel 34, lid 3 AVG geldt. Zij legt elk datalek vast, ook als een melding niet nodig is. Wij helpen haar daarbij. De termijn van 72 uur begint niet pas bij ons eindverslag. Bij een latere melding moet de organisatie de vertraging toelichten.
6. **Verslag.** Binnen tien werkdagen na kennisname sturen wij een schriftelijk verslag. Loopt het onderzoek nog, dan vermelden wij dat en vullen wij het verslag aan. Dit stelt eerdere meldingen niet uit.
7. **Leren.** Wij passen het systeem of de procedure aan, om herhaling te voorkomen.

12. Bewaren en verwijderen

Gegevens	Bewaartermijn
Gesprekken (vragen, antwoorden, opgestelde rapportages, de indeling naar onderwerp)	90 dagen, of de termijn die de organisatie instelt; een gesprek dat de functie uit bijlage 3 bij de verwerkersovereenkomst opvroeg, tot het onderzoek is afgerond (art. 5.5)
Documenten	Zolang de organisatie ze in Inora laat staan; binnen 30 dagen na verwijdering ook uit back-ups weg
Gebruikersaccounts	Zolang de gebruiker toegang heeft en tot 30 dagen daarna
Loggegevens	12 maanden, tenzij de overeenkomst eerder eindigt
Dienstmetingen (aantallen vragen en responstijden per gebruiker)	Per gebruiker 30 dagen; daarna alleen opgeteld per team van minstens vijf mensen
Bekwaamheidsdossier	Zolang de medewerker bij de organisatie werkt, plus 30 dagen; in die 30 dagen exporteert de organisatie het naar haar eigen personeelsdossier
Toetsset, alleen op schriftelijke opdracht van de organisatie	Tot de organisatie de opdracht intrekt, uiterlijk tot het einde van de overeenkomst; daarna binnen 30 dagen weg
Antwoordverslag (bronnen, versies, model, toets en datum per antwoord, en een kenmerk dat de medewerker bij het antwoord ziet)	2 jaar, bij Axiomatic; daarna binnen 30 dagen uit back-ups

Gegevens	Bewaartermijn
Back-ups	30 dagen
Alle gegevens na afloop van de overeenkomst	Naar keuze van de organisatie teruggeven of verwijderen; beschikbaar voor teruggave tot en met dag 30, tenzij eerder afgerond of om verwijdering gevraagd; actieve systemen, inclusief loggegevens en zoekindexen, leeg uiterlijk dag 30; back-ups leeg uiterlijk dag 60

Alleen een bewaarplicht uit het Unierecht of Nederlands recht kan een uitzondering op verwijdering rechtvaardigen. Wij melden dan welke gegevens, grond en termijn dat betreft, tenzij de wet dat verbiedt. De gegevens blijven beschermd zolang wij ze bewaren. Na verwijdering tijdens de looptijd kunnen kopieën nog maximaal 30 dagen in back-ups staan. Bij herstel passen wij verwijderingen opnieuw toe. Op verzoek bevestigen wij de verwijdering schriftelijk.

13. Verzoeken van overheden

Wij verstrekken gegevens van organisaties alleen aan een overheidsinstantie als het Unierecht of Nederlands recht ons daartoe verplicht, bijvoorbeeld op grond van een rechterlijk bevel, en dan niet meer dan nodig. Tenzij de wet het verbiedt, laten wij het de organisatie eerst weten. Tegen verzoeken zonder geldige wettelijke grondslag maken wij bezwaar.

Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.

14. Verantwoording

Voor de beoordeling door de organisatie:

- dit beveiligingsoverzicht;
- de verwerkersovereenkomst, met onderwerpen uit het model van de Brancheorganisaties Zorg, maar met eigen bepalingen;
- de lijst van subverwerkers;
- de controlematrix in paragraaf 15: elke beheersmaatregel van ISO 27001 en NEN 7510 en hoe wij die hebben ingericht, de basis voor uw verklaring van toepasselijkheid;

- een beschrijving van de verwerking, voor de gegevensbeschermingseffectbeoordeling (DPIA) van de organisatie.

Wij werken mee aan audits en inspecties door de organisatie of haar gemachtigde auditor over alle verplichtingen uit de verwerkersovereenkomst. Een reguliere audit vindt in beginsel eenmaal per jaar plaats. Extra controles blijven mogelijk waar nodig voor artikel 28 AVG, onder meer bij een incident, aanwijzingen van niet-naleving, een wezenlijke wijziging of een verzoek van de toezichthouder. De organisatie draagt de kosten van haar eigen auditor, tenzij de audit een wezenlijke tekortkoming aan onze kant aantoont.

15. Controlematrix

Ingericht volgens NEN 7510 en ISO 27001: elke beheersmaatregel uit bijlage A van ISO/IEC 27001:2022 en de maatregelen die NEN 7510 voor de zorg toevoegt, met hoe Axiomatic die voor Inora heeft ingericht en de status per regel.

Elke maatregel, met hoe die is ingericht, staat in de Controlematrix in dit dossier.

16. Contact

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

AXIOMATIC

Controlematrix

Inora, ingericht volgens NEN 7510 en ISO 27001

Versie 1.3, 9 november 2026

Elke beheersmaatregel uit bijlage A van ISO/IEC 27001:2022, zoals NEN 7510 die overneemt, en de acht maatregelen die NEN 7510 voor de zorg toevoegt, met hoe Axiomatic die voor Inora heeft ingericht. “Bij AWS” betekent dat de cloudleverancier de maatregel uitvoert, met zijn eigen auditrapporten als bewijs. Dit document is de basis voor uw verklaring van toepasselijkheid bij uw eigen beoordeling van Inora als leverancier.

Fysieke maatregelen in de datacentra liggen bij de cloudleverancier, Amazon Web Services EMEA SARL, in de regio Europa (Ierland). Wie verder gegevens verwerkt, staat op axiomatic.digital/vertrouwen/subverwerkers.

Organisatorisch (37)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.1	Beleidsregels voor informatiebeveiliging	Het beveiligingsbeleid en het beveiligings-overzicht leggen vast hoe Inora is beveiligd, en beide zijn openbaar. Iedereen bij Axiomatic leest en tekent de beveiligingsregels bij de start en daarna elk jaar opnieuw. De directeur keurt het beleid goed en herziet het elk jaar en na elk ernstig beveiligingsincident.	▪ Ingericht
5.2	Rollen en verantwoorde-lijkheden bij informatiebeveiliging	De directeur is verantwoordelijk voor beveiliging en privacy binnen Axiomatic. Het beveiligings-overzicht noemt wie bij de productieomgeving kan en wie niet.	▪ Ingericht
5.3	Functiescheiding	Geen wijziging gaat in productie zonder beoordeling door een tweede engineer. Wie organisaties bij de implementatie begeleidt, heeft geen toegang tot de productieomgeving of tot hun gegevens.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.4	Managementverantwoordelijkheden	De directie eist van iedereen dat hij de beveiligingsregels bij de start en elk jaar tekent, en draagt de verantwoordelijkheid voor beveiliging en privacy zelf.	▪ Ingericht
5.5	Contact met overheidsinstanties	Bij een datalek helpen wij de organisatie met haar melding bij de Autoriteit Persoonsgegevens. Een overheidsverzoek beantwoorden wij alleen als het Unierecht of Nederlands recht ons verplicht, met niet meer dan nodig en, tenzij de wet het verbiedt, nadat de organisatie het weet.	▪ Ingericht
5.6	Contact met speciale belangengroepen	Wij volgen de beveiligingsadviezen van het NCSC en Z-CERT en de beveiligingsmeldingen van elk bouwblok waarop Inora draait.	▪ Ingericht
5.7	Informatie en analyses over dreigingen	Met de adviezen uit 5.6 beoordelen wij elke maand welke dreigingen Inora raken, en leggen dat vast. Bekende kwetsbaarheden in de bibliotheken worden automatisch gevolgd.	▪ Ingericht
5.8	Informatiebeveiliging in projectmanagement	Elke implementatie en elke nieuwe functie begint met de beveiligingsvragen schriftelijk beantwoord: welke gegevens, wie erbij kan, welke leverancier.	▪ Ingericht
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Een register noemt elk systeem, elke leverancier, elke gegevensopslag en elke laptop, met een eigenaar, en wordt elk kwartaal nagelopen.	▪ Ingericht
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	De beveiligingsregels die iedereen tekent, zeggen hoe informatie en laptops gebruikt mogen worden. Gegevens van organisaties staan nooit op een laptop.	▪ Ingericht
5.11	Retourneren van bedrijfsmiddelen	Vertrekt iemand, dan komt de laptop op de laatste werkdag terug en wordt hij gewist. De toegang vervalt dezelfde dag.	▪ Ingericht
5.12	Classificeren van informatie	Alles wat gebruikers in Inora typen, geldt als gezondheidsgegeven en wordt zo beschermd. De documenten van de organisatie gelden als intern.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.13	Labelen van informatie	Elke omgeving, opslag en zoekindex draagt in de infrastructuur het label van haar organisatie en haar gegevensklasse.	▪ Ingericht
5.14	Overdragen van informatie	Al het verkeer van en naar Inora, en tussen de onderdelen ervan, is versleuteld met TLS 1.2 of hoger. Wat wij met gegevens doen en met wie, staat in de verwerkersovereenkomst.	▪ Ingericht
5.15	Toegangsbeveiliging	De organisatie bepaalt welke groepen medewerkers toegang krijgen en wie beheerder is. Bij de productieomgeving kunnen alleen de engineers die Inora bouwen, elk bij naam.	▪ Ingericht
5.16	Identiteitsbeheer	Medewerkers loggen in met hun eigen account via het identiteitsbeheer van de organisatie, met SAML of OpenID Connect; SCIM maakt accounts aan en sluit ze af. Schakelt de organisatie een account daar uit, dan kan die persoon niet meer inloggen. Gedeelde accounts zijn er niet.	▪ Ingericht
5.17	Beheren van authenticatie-informatie	Met single sign-on bewaart Inora geen wachtwoorden. Beheertoegang tot de productie-omgeving vraagt een fysieke beveiligingssleutel, en sleutels en certificaten van diensten staan in een sleutelkluis, nooit in de broncode.	▪ Ingericht
5.18	Toegangsrechten	Elk kwartaal controleren wij de toegangsrechten. Vertrekt iemand, dan vervalt de toegang dezelfde dag.	▪ Ingericht
5.19	Informatiebeveiliging in leveranciersrelaties	Wij werken met zo min mogelijk subverwerkers: voor Inora Amazon Web Services, en Microsoft (Azure OpenAI, EU). Wij blijven verantwoordelijk voor wat onze leveranciers doen.	▪ Ingericht
5.20	Adresseren van informatie-beveiliging in leveranciersovereen-komsten	Elke subverwerker heeft een overeenkomst getekend met verplichtingen die niet zwakker zijn dan die in onze verwerkersovereenkomst.	▪ Ingericht
5.21	Beheren van informatiebe-veiliging in de ICT-keten	Inora draait op open bouwblokken en het taalmodel is uitwisselbaar, zodat Inora van geen enkele leverancier afhangt. De bibliotheken waarop het draait, worden gecontroleerd op bekende kwetsbaarheden.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Een nieuwe subverwerker melden wij 30 dagen vooraf. De organisatie kan bezwaar maken. Vinden wij samen geen oplossing, dan mag zij de overeenkomst beëindigen voor het deel dat zonder de nieuwe subverwerker niet kan worden geleverd, zonder kosten.	▪ Ingericht
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Inora draait bij Amazon Web Services EMEA SARL in de regio Europa (Ierland), het taalmodel via het EU-inferentieprofiel van Amazon Bedrock of via Azure OpenAI in de EU; het systeem kiest het model. Niemand traint modellen met deze gegevens. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model, en Azure OpenAI draait met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens, zodat Microsoft geen vragen of antwoorden bewaart en geen medewerker van Microsoft ze leest.	▪ Ingericht
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Een vastgelegde incidentprocedure in zeven stappen: ontdekken, indammen, beoordelen, melden, ondersteunen, verslag en leren.	▪ Ingericht
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Elke gebeurtenis wordt beoordeeld op welke organisaties, gegevens en mensen zij raakt, en ingedeeld in vier ernstklassen, van kritiek tot laag, zoals Kwetsbaarheid melden ze beschrijft.	▪ Ingericht
5.26	Reageren op informatiebeveiligingsincidenten	Een datalek of een vermoeden daarvan melden wij uiterlijk 24 uur na kennisname aan de organisatie, met wat bekend is. Binnen tien werkdagen volgt een schriftelijk verslag.	▪ Ingericht
5.27	Leren van informatiebeveiligingsincidenten	Elk incident onderzoeken wij zonder schuldvraag, met de oorzaak in het systeem, en wij passen het systeem of de procedure aan om herhaling te voorkomen.	▪ Ingericht
5.28	Verzamelen van bewijsmateriaal	Bij een incident leggen wij een momentopname van de getroffen omgeving vast voordat er iets verandert, met wie haar nam en wanneer. De logging is onveranderbaar (5.33).	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.29	Informatiebeveiliging tijdens een verstoring	De herstelprocedure staat op papier, zodat elke engineer haar alleen kan uitvoeren. Na een herstel passen wij verwijderingen opnieuw toe.	▪ Ingericht
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Elke dag een back-up, elk kwartaal een hersteltest, ten hoogste 24 uur gegevensverlies. Een herstel uit back-up duurt ten hoogste 8 uur. Ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht.	▪ Ingericht
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	De AVG, de UAVG en de AI-verordening zijn in de gepubliceerde beleidsstukken op Inora betrokken. De verwerkersovereenkomst volgt artikel 28 AVG.	▪ Ingericht
5.32	Intellectuele-eigendomsrechten	De protocollen en het handboek blijven van de organisatie die ze schreef. Voor bronnen van anderen, zoals landelijke richtlijnen, geldt de licentie van hun uitgever.	▪ Ingericht
5.33	Beschermen van registraties	Logging wordt 12 maanden in de EU bewaard en kan door de applicatie niet worden gewijzigd. Facturen en de stukken erachter bewaren wij zeven jaar, zoals de fiscale wet vraagt.	▪ Ingericht
5.34	Privacy en bescherming van persoonsgegevens	De organisatie is verwerkingsverantwoordelijke, wij zijn verwerker. Niemand in de organisatie leest een gesprek van een medewerker, en geen model traint op de gegevens.	▪ Ingericht
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De organisatie of haar auditor controleert elke verplichting uit de verwerkersovereenkomst, in beginsel eenmaal per jaar.	▪ Ingericht
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Elk jaar toetsen wij deze matrix aan wat in productie draait; een afwijking wordt hersteld of vastgelegd.	▪ Ingericht
5.37	Gedocumenteerde bedieningsprocedures	De incidentprocedure en de herstelprocedure staan op papier, zodat elke engineer haar alleen kan uitvoeren.	▪ Ingericht

Mensgericht (8)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
6.1	Screening	Iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).	▪ Ingericht
6.2	Arbeidsovereenkomst	Iedereen tekent een geheimhoudingsverklaring die ook na vertrek blijft gelden, en de beveiligingsregels, bij de start en daarna elk jaar.	▪ Ingericht
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Twee keer per jaar oefent het team met phishing en met het omgaan met zorggegevens. Iedereen tekent de beveiligingsregels bij de start en elk jaar.	▪ Ingericht
6.4	Disciplinaire procedure	De beveiligingsregels noemen wat er gebeurt bij een overtreding, van een gesprek tot het intrekken van toegang en ontslag.	▪ Ingericht
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	De geheimhouding blijft na vertrek gelden, en de toegang vervalt dezelfde dag.	▪ Ingericht
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend, zoals artikel 30, lid 4 UAVG vraagt van wie gezondheidsgegevens verwerkt zonder eigen beroepsgeheim.	▪ Ingericht
6.7	Werken op afstand	Werklaptops hebben volledige schijfversleuteling, een firewall en automatische beveiligingsupdates, en vergrendelen na enkele minuten. Gegevens van organisaties staan nooit op een laptop.	▪ Ingericht
6.8	Melden van informatiebeveiligingsgebeurtenissen	Een verloren of gestolen laptop melden wij dezelfde dag. Onderzoekers melden een kwetsbaarheid per mail en krijgen binnen drie werkdagen een ontvangstbevestiging.	▪ Ingericht

Fysiek (14)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
7.1	Fysieke beveiligingszones	Inora draait alleen in datacenters van Amazon Web Services in de EU; hun fysieke beveiliging ligt bij AWS, volgens zijn eigen ISO/IEC 27001- en SOC 2-rapporten. Op het kantoor van Axiomatic staan geen gegevens van organisaties.	▣ Ingericht bij AWS
7.2	Fysieke toegangsbeveiliging	Axiomatic heeft geen eigen serverruimte; niemand van Axiomatic komt in een datacenter. Wij bereiken Inora alleen op afstand, met een persoonlijk account en een fysieke beveiligings-sleutel (de datacenters zelf: 7.1).	▪ Ingericht
7.3	Beveiligen van kantoren, ruimten en faciliteiten	De ruimten waar gegevens van organisaties staan, zijn die van AWS. Een kantoor van Axiomatic bevat geen gegevens van organisaties.	▣ Ingericht bij AWS
7.4	Monitoren van de fysieke beveiliging	De datacenters worden door AWS bewaakt, zoals zijn eigen auditrapporten beschrijven.	▣ Ingericht bij AWS
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Brand, water, stroom en klimaat in de datacenters zijn de verantwoordelijkheid van AWS. Back-ups staan apart van de productie, versleuteld, in de EU.	▣ Ingericht bij AWS
7.6	Werken in beveiligde zones	Het werk in de beveiligde zones van de datacenters doet AWS; Axiomatic werkt er niet.	▣ Ingericht bij AWS
7.7	‘Clear desk’ en ‘clear screen’	Laptops vergrendelen na enkele minuten zonder gebruik. Gegevens van organisaties staan nooit op een laptop, en dus ook nooit op een bureau.	▪ Ingericht
7.8	Plaatsen en beschermen van apparatuur	De servers van Inora zijn die van AWS, door AWS geplaatst en beschermd.	▣ Ingericht bij AWS
7.9	Beveiligen van bedrijfs-middelen buiten het terrein	Laptops hebben volledige schijfversleuteling. Een verloren of gestolen laptop melden wij dezelfde dag, en zijn toegang trekken wij in.	▪ Ingericht
7.10	Opslagmedia	Opslag met gegevens van organisaties is die van AWS, versleuteld met AES-256. De schijven van laptops zijn volledig versleuteld.	▣ Ingericht bij AWS
7.11	Nutsvoorzieningen	Stroom, koeling en netwerk van de datacenters zijn de verantwoordelijkheid van AWS.	▣ Ingericht bij AWS

Nr.	Beheersmaatregel	Zo is het ingericht	Status
7.12	Beveiligen van bekabeling	De bekabeling van de datacenters is de verantwoordelijkheid van AWS. Al het verkeer van Inora is versleuteld, ook over die kabels.	▣ Ingericht bij AWS
7.13	Onderhoud van apparatuur	AWS onderhoudt de apparatuur in zijn datacenters. Laptops installeren beveiligingsupdates automatisch.	▣ Ingericht bij AWS
7.14	Veilig verwijderen of hergebruiken van apparatuur	Schijven met gegevens van organisaties zijn die van AWS, die ze volgens zijn eigen gecontroleerde procedure wist of vernietigt. Op laptops staan geen gegevens van organisaties.	▣ Ingericht bij AWS

Technologisch (34)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.1	‘User endpoint devices’	Werklaptops: volledige schijfversleuteling, firewall, automatische updates en schermvergrendeling. Medewerkers van de organisatie gebruiken Inora in de browser, ingelogd via het eigen identiteitsbeheer van de organisatie.	▪ Ingericht
8.2	Speciale toegangsrechten	Beheertoegang tot de productieomgeving hebben alleen de engineers die Inora bouwen, met een persoonlijk account, multifactorauthenticatie en een fysieke beveiligingssleutel. Elke toegang wordt vastgelegd.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.3	Beperking toegang tot informatie	Een vraag binnen de ene organisatie kan alleen de documenten van die organisatie bereiken. Niemand in de organisatie leest een gesprek van een medewerker. Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die de organisatie aanwijst, voor een incident of een klacht, of bij een wettelijke vordering (art. 5.6); elke inzage wordt vastgelegd en de medewerker hoort ervan, tenzij de wet dat verbiedt. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoord-verslag, nooit een gesprek. Voor de teamver-slagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, zonder namen; geen mens leest mee (art. 5.6).	▪ Ingericht
8.4	Toegangsbeveiliging op broncode	De broncode is alleen bereikbaar met een persoonlijk account met multifactorauthenticatie, en elke wijziging wordt door een tweede engineer beoordeeld.	▪ Ingericht
8.5	Beveiligde authenticatie	Inloggen loopt via het eigen identiteitsbeheer van de organisatie, met SAML of OpenID Connect, en haar eigen regels voor multifactorauthenticatie; SCIM maakt accounts aan en sluit ze af. Bij Entra ID geeft de toestemming Inora alleen openid, profile, email en User.Read, gedelegeerd en alleen-lezen; geen toegang tot mail, bestanden, Teams of SharePoint. Inora leest alleen de groepen die de organisatie aan de app toewijst, zodat de claim nooit overloopt. Een sessie eindigt uiterlijk acht uur nadat zij begon.	▪ Ingericht
8.6	Capaciteitsbeheer	Belasting, opslag en modelcapaciteit worden per omgeving gemeten, met een melding voordat een grens wordt bereikt.	▪ Ingericht
8.7	Bescherming tegen malware	Elk document dat in Inora komt, wordt op malware gescand voordat het in de zoekindex komt. Laptops draaien de malwarebescherming van het besturingssysteem.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.8	Beheer van technische kwetsbaarheden	De bibliotheken van Inora worden automatisch gecontroleerd op bekende kwetsbaarheden. Kritieke beveiligingsupdates voeren wij binnen 72 uur door, andere binnen 30 dagen.	▪ Ingericht
8.9	Configuratiebeheer	De infrastructuur wordt als code vastgelegd en beoordeeld als software, langs dezelfde tweede engineer als een wijziging in Inora.	▪ Ingericht
8.10	Wissen van informatie	Gesprekken verdwijnen na 90 dagen, of na de termijn die de organisatie instelt; een gesprek dat de functie uit bijlage 3 bij de verwerkersovereenkomst opvroeg, blijft tot het onderzoek is afgerond (art. 5.5). Na de overeenkomst zijn de actieve systemen uiterlijk op dag 30 leeg en de back-ups op dag 60, schriftelijk bevestigd.	▪ Ingericht
8.11	Maskeren van gegevens	Ontwikkelen en testen gebeurt zonder gegevens van organisaties. De metingen die Axiomatic ziet, bevatten geen namen en geen inhoud van documenten, vragen of antwoorden.	▪ Ingericht
8.12	Voorkomen van gegevenslekken (‘data leakage prevention’)	Een vraag kan alleen de documenten van de eigen organisatie bereiken. Gegevens van organisaties komen nooit op een laptop en nooit in de AI-hulpmiddelen waarmee wij software schrijven.	▪ Ingericht
8.13	Back-up van informatie	Elke dag een back-up van elke omgeving, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland). Elk kwartaal zetten wij er een terug om te controleren of die werkt.	▪ Ingericht
8.14	Redundantie van informatieverwerkende faciliteiten	Inora draait verdeeld over meerdere beschikbaarheidszones van de regio Europa (Ierland), zodat het uitvallen van één datacenter het niet stillegt. Ook de opgeslagen gegevens staan bij AWS verspreid over meerdere zones.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.15	Logging	Inora legt inlogmomenten, beheerhandelingen en elke toegang door medewerkers van Axiomatic vast, 12 maanden lang. Op verzoek krijgt een organisatie de beveiligingslogging van haar omgeving, opgeteld per team van minstens vijf mensen en per dag, en elke toegang door Axiomatic; een dag met minder dan vijf inlogs staat er als '<5'. Inlogmomenten en IP-adressen van één medewerker gaan nooit naar de organisatie. Bij een beveiligingsincident onderzoekt Axiomatic het logboek zelf en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen.	▪ Ingericht
8.16	Monitoren van activiteiten	Wij krijgen een melding bij herhaald mislukt inloggen, ongewoon verkeer, fouten en onbeschikbaarheid.	▪ Ingericht
8.17	Kloksynchronisatie	Elke server neemt zijn tijd van de tijdsdienst van de cloudleverancier, zodat de logging van alle onderdelen op de seconde gelijkloopt.	▪ Ingericht
8.18	Gebruik van speciale systeemhulpmiddelen	Beheerhulpmiddelen die de applicatie kunnen omzeilen, bereiken de productieomgeving alleen via de persoonlijke accounts van de engineers, met een fysieke beveiligingssleutel. Elke toegang wordt vastgelegd.	▪ Ingericht
8.19	Installeren van software op operationele systemen	Software komt alleen als beoordeelde release via de uitrolstraat in productie; niemand installeert met de hand iets op een draaiende server.	▪ Ingericht
8.20	Beveiliging netwerkcomponenten	Al het verkeer naar Inora en tussen de onderdelen ervan gebruikt TLS 1.2 of hoger; oudere protocollen worden geweigerd.	▪ Ingericht
8.21	Beveiliging van netwerkdiensten	Inora is alleen bereikbaar via de load balancer van AWS, achter een webapplicatiefirewall die bekende aanvalspatronen tegenhoudt.	▪ Ingericht
8.22	Netwerksegmentatie	Elke organisatie heeft een eigen omgeving, gescheiden in de infrastructuur en niet alleen in de software. Ontwikkelen en testen gebeurt apart van de productie.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.23	Toepassen van webfilters	Werklaptops filteren het webverkeer op DNS-niveau en blokkeren bekende kwaadaardige domeinen.	▪ Ingericht
8.24	Gebruik van cryptografie	TLS 1.2 of hoger tijdens transport, AES-256 bij opslag voor databases, documentopslag, zoekindexen en back-ups. De sleutels staan in AWS Key Management Service, in de EU; elk gebruik wordt vastgelegd. Geheimen staan in een sleutelkluis.	▪ Ingericht
8.25	Beveiligen tijdens de ontwikkelcyclus	Elke wijziging wordt door een tweede engineer beoordeeld, met de OWASP Top 10 als checklist. Geeft de organisatie daarvoor een schriftelijke opdracht, na instemming van haar ondernemingsraad waar zij er een heeft, dan wordt elke nieuwe versie getest op haar toetsset, haar eigen vragen en gemarkeerde antwoorden ontdaan van namen, voordat haar medewerkers die versie zien.	▪ Ingericht
8.26	Toepassingsbeveiligingseisen	Naast de OWASP Top 10 telt wat eigen is aan Inora als beveiligingsfout: een antwoord buiten de bronnen van de organisatie, of een organisatie die bij een andere komt. De ernstklassen op Kwetsbaarheid melden noemen ze.	▪ Ingericht
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Per organisatie een eigen database, documentopslag en zoekindex; geen gedeelde database met organisaties gescheiden door een kolom. Het taalmodel is uitwisselbaar, en de verwerking blijft in de EU.	▪ Ingericht
8.28	Veilig coderen	De OWASP Top 10 is de checklist bij elke beoordeling. Geheimen staan nooit in de broncode, en bibliotheken worden gecontroleerd op bekende kwetsbaarheden.	▪ Ingericht
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Geeft de organisatie daarvoor een schriftelijke opdracht, na instemming van haar ondernemingsraad waar zij er een heeft, dan wordt elke nieuwe versie getest op haar toetsset, haar eigen vragen en gemarkeerde antwoorden ontdaan van namen, voordat zij live gaat.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.30	Uitbestede systeemontwikkeling	Inora wordt gebouwd door de eigen engineers van Axiomatic. Geen externe kracht heeft toegang tot de productieomgeving of tot gegevens van organisaties.	▪ Ingericht
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkelen en testen gebeurt in een aparte omgeving, zonder gegevens van organisaties.	▪ Ingericht
8.32	Wijzigingsbeheer	Elke wijziging wordt door een tweede engineer beoordeeld voordat zij in productie gaat. Gepland onderhoud kondigen wij vooraf aan, en een functie waarop de organisatie rekent, verdwijnt niet zonder aankondiging.	▪ Ingericht
8.33	Testgegevens	Testgegevens bevatten geen gegevens van organisaties; ontwikkelen en testen gebeurt zonder.	▪ Ingericht
8.34	Bescherming van informatiesystemen tijdens audits	Audits en tests op productie worden vooraf afgesproken, waar het kan alleen-lezen en buiten de drukste uren.	▪ Ingericht

Zorg (NEN 7510) (8)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.38	Analyse en specificatie van informatiebeveiligingseisen	Voor elke functie gelden vooraf de OWASP Top 10 en de fouten die eigen zijn aan Inora: een antwoord buiten de bronnen, of een organisatie die bij een andere komt.	▪ Ingericht
5.39	Zorgontvangers op unieke wijze identificeren	Inora registreert geen zorgontvangers en kent dus geen dubbele registraties; de unieke identificatie en het samenvoegen gebeuren in het ECD van de organisatie. Inora vraagt niet om een burgerservicenummer.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.40	Validatie van getoonde/geprinte gegevens	Inora registreert geen zorgontvangers. Een rapportage over een cliënt gaat pas na akkoord het dossier in van de cliënt die de zorgmedewerker in het ECD open heeft; daar identificeert de organisatie de cliënt. Elke zin die op een bron van de organisatie rust, draagt een markering die het document en de passage toont.	▪ Ingericht
5.41	Openbaar beschikbare gezondheidsinformatie	Openbare bronnen die de organisatie aanwijst, zoals landelijke richtlijnen, leest Inora zoals ze zijn uitgegeven, onder de licentie van hun uitgever, en elk antwoord toont de bron waarop het rust.	▪ Ingericht
5.42	Communicatie in noodsituaties	Een storing die Inora onbruikbaar maakt, meldt de organisatie via support@axiomatic.digital, dag en nacht; reactie binnen een uur. Bij een datalek hoort haar contactpersoon het uiterlijk 24 uur na kennisname. Het kanaal en een tweede contactpersoon beproeven wij elk jaar met de contactpersoon van de organisatie.	▪ Ingericht
5.43	Incidenten extern melden	Wij melden een datalek uiterlijk 24 uur na kennisname aan de organisatie en helpen haar met haar melding bij de Autoriteit Persoonsgegevens, die waar mogelijk binnen 72 uur moet.	▪ Ingericht
6.9	Managementtraining	De directie volgt elk jaar een training in de plichten die de Cyberbeveiligingswet en NEN 7510 aan het bestuur stellen.	▪ Ingericht
8.35	Zero trust-beginselen	Geen toegang rust op een netwerklocatie: elke gebruiker logt in via de eigen identiteitsdienst van de organisatie, elke beheertoegang met een persoonlijk account en een fysieke sleutel, en elke toegang wordt vastgelegd.	▪ Ingericht

Vragen over deze matrix: security@axiomatic.digital.

AXIOMATIC

Subverwerkers

Axiomatic B.V. en Inora

Versie 1.6, 11 november 2026

Een subverwerker is een bedrijf dat wij inschakelen en dat persoonsgegevens uit Inora verwerkt in opdracht van een zorgorganisatie. Wij gebruiken er zo weinig mogelijk. Met elke subverwerker hebben wij een overeenkomst gesloten met verplichtingen die niet lichter zijn dan die in onze verwerkersovereenkomst.

Inora

Alle subverwerkers van Inora verwerken gegevens in de Europese Unie.

Subverwerker	Dienst	Gegevens	Locatie	Buiten de EER
Amazon Web Services EMEA SARL, Luxemburg	Hosting: applicatie, database, documentopslag, zoekindex en back-ups (Amazon Web Services)	Alle gegevens in Inora	Regio Europa (Ierland), eu-west-1	Nee

Subverwerker	Dienst	Gegevens	Locatie	Buiten de EER
Amazon Web Services EMEA SARL, Luxemburg	Taal- en embeddingmodellen (Amazon Bedrock, EU-inferentieprofiel)	Vragen, ook ingesproken, en gevonden passages tijdens het antwoord, waarbij het model in dezelfde stap het onderwerp indeelt voor de teamverslagen; op schriftelijke opdracht de inhoud van de toetsset, om de namen te verwijderen; documentpassages bij het opbouwen van de zoekindex; niet gebruikt voor training; Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model	Regio's van Amazon Web Services in de EU	Nee
Microsoft Ireland Operations Limited, Dublin	Taalmodellen (Azure OpenAI, EU-regio); het systeem kiest per taak het model	Vragen, ook ingesproken, en gevonden passages tijdens het antwoord, waarbij het model in dezelfde stap het onderwerp indeelt voor de teamverslagen; op schriftelijke opdracht de inhoud van de toetsset, om de namen te verwijderen; niet gebruikt voor training	Een Azure-regio in de EU	Nee

Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU, of op uw eigen servers binnen uw netwerk. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek.

Axiomatic draait Azure OpenAI met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).

De moederbedrijven van Amazon Web Services en Microsoft, Amazon.com, Inc. en Microsoft Corporation, zijn Amerikaans en staan allebei op de lijst van het EU-VS-kader voor gegevensbescherming (Data Privacy Framework). Ons privacyverklaring legt uit wat dat betekent.

Draait Inora voor een organisatie elders, op haar eigen servers of buiten de EU, dan noemt haar verwerkersovereenkomst de leveranciers en regio's van die inrichting.

Voor ons eigen werk

Deze diensten ondersteunen Axiomatic als bedrijf. Zij krijgen nooit gegevens uit Inora en zijn dus geen subverwerkers in de zin van de verwerkersovereenkomst. Wij noemen ze omdat zij persoonsgegevens verwerken van bezoekers van de website en van mensen die contact met ons opnemen.

Verwerker	Dienst	Gegevens	Locatie
Amazon Web Services EMEA SARL, Luxemburg	Hosting van de website axiomatic.digital (Amazon S3 en Amazon CloudFront)	Technische verzoekgegevens: IP-adres, pagina, tijdstip, browser	Bestanden in regio Europa (Ierland); levering via het wereldwijde netwerk van CloudFront
Amazon Web Services EMEA SARL, Luxemburg	De AI-scan: opslag van de verstuurde antwoorden (Amazon DynamoDB), de verwerking (AWS Lambda) en de e-mail aan ons (Amazon SES)	Antwoorden, uitkomst, taal, tijdstip en het e-mailadres als u dat invult	Regio Europa (Ierland)

Verwerker	Dienst	Gegevens	Locatie
Google Cloud EMEA Limited, Dublin, Ierland	E-mail, documenten en agenda (Google Workspace)	Correspondentie en contact-gegevens. Meldingen noemen de soorten gegevens en het aantal betrokkenen, nooit gegevens uit Inora.	Datacenters van Google, ook buiten de EU
PostHog, Inc., Verenigde Staten	Webanalyse en opnamen van bezoeken aan de website	Bekeken pagina's, klikken, een opname van het bezoek met wat in formulieren wordt getypt, herkomst, IP-adres en browser; een kopie van de verstuurde AI-scan; na een formulier of een persoonlijke link naam, e-mailadres, functie en organisatie	EU-cloud van PostHog, in Duitsland
Intercom R&D Unlimited Company, Ierland	De chat op de website	IP-adres, browser, de bekeken pagina, het gesprek; na een formulier naam en e-mailadres	Verenigde Staten
IPinfo, Inc., Verenigde Staten	De organisatie bij een IP-adres	Alleen het IP-adres	Verenigde Staten

PostHog, Intercom en IPinfo krijgen nooit gegevens uit Inora; zij dienen alleen de website, zoals onze privacyverklaring beschrijft. De Amerikaanse moederbedrijven, Amazon.com, Inc. en Google LLC, en PostHog, Inc. en Intercom, Inc. staan op de lijst van het EU-VS-kader voor gegevensbescherming (Data Privacy Framework).

Wijzigingen

Een nieuwe of vervangende subverwerker voor Inora melden wij per e-mail aan de contactpersoon van elke klant, ten minste 30 dagen voordat hij gegevens gaat verwerken. Een klant kan binnen die termijn bezwaar maken. Tegelijk passen wij deze lijst en de datum bovenaan aan.

Vragen: privacy@axiomatic.digital.

AXIOMATIC

Privacydossier

Inora, voor de functionaris gegevensbescherming

Dit dossier volgt de verwerkersovereenkomst, de lijst van subverwerkers versie 1.6, het beveiligingsoverzicht versie 1.4 en de controlematrix versie 1.3, en de privacyverklaring. Bij verschil gaan de artikelen van de ondertekende verwerkersovereenkomst voor. De verwerkersovereenkomst ontvangt u bij het voorstel.

Versie 1.16, 11 november 2026

1. Wat dit dossier regelt

Dit dossier is voor de functionaris gegevensbescherming (FG) of de privacyfunctionaris van een zorgorganisatie die Inora beoordeelt. Het beantwoordt één vraag: blijven onze gegevens binnen de EU? Ja, uw gegevens blijven binnen de EU.

Wat hier staat, is ingevuld door Axiomatic: de beschrijving van de verwerking, de doeleinden, de feiten voor de grondslag, de risico's met hun maatregelen en de DPIA, kop voor kop. Dit dossier is het ene DPIA-document van Inora, en het is openbaar. Wat van u blijft, staat er telkens apart bij onder **Uw deel**: de grondslag, de omvang, de weging van de risico's voor uw organisatie en uw eigen maatregelen.

2. De verwerking beschreven

2.1 Rollen

Partij	Rol	Artikel	Wat zij doet
Uw organisatie	Verwerkingsverant-woordelijke	art. 4, onder 7 AVG	Bepaalt waarvoor Inora dient, welke bronnen erin staan, wie ermee werkt en hoe lang gesprekken blijven. Stelt de grondslag vast, voert de DPIA uit, meldt datalekken bij de Autoriteit Persoonsgegevens.
Axiomatic B.V., Delft (KvK 97816825)	Verwerker	art. 28 AVG	Bouwt, implementeert en beheert Inora, alleen op uw gedocumenteerde instructie. Staat tegenover u volledig in voor elke subverwerker.
Amazon Web Services EMEA SARL, Luxemburg	Subverwerker	art. 28, lid 4 AVG	Hosting in de regio Europa (Ierland); het taal- en embeddingmodel via Amazon Bedrock met het EU-inferentieprofiel. Gebonden aan plichten die niet lichter zijn dan die van Axiomatic.
Microsoft Ireland Operations Limited, Dublin	Subverwerker	art. 28, lid 4 AVG	Taalmodellen via Azure OpenAI in de EU-regio; het systeem kiest het model. Gebonden aan plichten die niet lichter zijn dan die van Axiomatic.

Eén partij bouwt, implementeert en beheert Inora. Er is geen implementatiepartner en er zijn geen andere subverwerkers voor Inora dan deze twee.

De moederbedrijven van de subverwerkers zijn Amerikaans: Amazon.com, Inc. (Seattle) en Microsoft Corporation (Redmond). Beide staan op de lijst van het EU-VS Data Privacy Framework. Axiomatic geeft geen persoonsgegevens door buiten de EU. Opslag in de EU sluit een verzoek van een buitenlandse overheid niet uit; zie §5, risico R4.

2.2 Het register van verwerkingen

Hieronder staat uw register (art. 30, lid 1 AVG), ingevuld uit het register dat Axiomatic als verwerker bijhoudt (art. 30, lid 2 AVG). Het algemene doel: zorgmedewerkers antwoord geven uit de eigen bronnen van de organisatie, en rapportages laten opstellen in haar format. Elke verwerking hieronder noemt haar eigen doel, en geen ander.

- **Verwerker:** Axiomatic B.V., Delft (KvK 97816825); functionaris gegevensbescherming: een externe FG, bereikbaar via fg@axiomatic.digital (art. 30, lid 2, onder a AVG).
- **Ontvangers:** Axiomatic B.V. (verwerker); Amazon Web Services EMEA SARL en Microsoft Ireland Operations Limited (subverwerkers); per team de teamleider en de ondernemingsraad.
- **Beveiliging:** bijlage 2 bij de verwerkersovereenkomst.

Nr.	Gegevens	Van wie	Waarvoor	Waar	Hoe lang	Grondslag
V1	Documenten: protocollen, richtlijnen, werkafspraken, het kwaliteitshandboek, met namen van auteurs en eigenaren	Medewerkers, als auteur of eigenaar	Doorzoeken en als bron tonen	Eigen opslag en zoekindex, Europa (Ierland); embedding via Amazon Bedrock in de EU	Zolang u het document laat staan; uit back-ups binnen 30 dagen	Art. 6 AVG: door u in te vullen
V2	Vragen, getypt of ingesproken, antwoorden en rapportages (SBAR, SOEP); kunnen gezondheidsgegevens van cliënten bevatten	Medewerkers; de cliënten over wie zij vragen	Antwoord uit uw bronnen, rapportage in uw format; per gesprek het onderwerp indelen voor de teamverslagen, ingebouwd	Europa (Ierland); het model in de EU via Amazon Bedrock of Azure OpenAI	90 dagen, of de termijn die u instelt; een gesprek dat de functie uit bijlage 3 opvroeg, tot het onderzoek is afgerond.	Art. 6 AVG; art. 9, lid 2, onder h AVG met art. 30, lid 3, onder a UAVG: door u in te vullen
V3	Accounts: naam, zakelijk e-mailadres, unieke code en groepen uit uw identiteitsbeheer, via single sign-on en SCIM	Medewerkers met toegang	Inloggen en toegang per rol	Europa (Ierland)	Zolang de toegang duurt, plus 30 dagen	Art. 6 AVG: door u in te vullen
V4	Logboek: inlogmomenten, beheerhandelingen, IP-adressen, tijdstippen, elke toegang door Axiomatic. Dossiertoegang staat in V11	Medewerkers van u en van Axiomatic	Beveiliging, onderzoek van incidenten, verantwoording; op verzoek krijgt u de logging alleen opgeteld per team van minstens vijf mensen en per dag, inlogmomenten en IP-adressen van één medewerker nooit	Europa (Ierland)	12 maanden	Art. 6 AVG: door u in te vullen
V5	Ondersteuning en implementatie: alleen de documenten die u Axiomatic vraagt in te zien; een gesprek van een medewerker alleen volgens VWO art. 5.5; geen kopieën buiten uw omgeving	Medewerkers; de cliënten over wie zij vragen	Vragen oplossen, de implementatie begeleiden	Europa (Ierland), in uw eigen omgeving	De termijn van de verwerking die het betreft	De grondslag van die verwerking, met art. 9, lid 2, onder h AVG met art. 30, lid 3, onder a UAVG, waar nodig: door u in te vullen

Nr.	Gegevens	Van wie	Waarvoor	Waar	Hoe lang	Grondslag
V6	Dienstmetingen: aantallen vragen en responstijden per gebruiker, zonder inhoud of namen	Medewerkers met toegang	Alleen uw eigen omgeving beheren en problemen daarin verhelpen; nooit per medewerker naar u	Europa (Ierland)	Per gebruiker 30 dagen, daarna alleen opgeteld per team van minstens vijf mensen	Art. 6 AVG: door u in te vullen
V7	Bekwaamheids-dossier in Inora Matrix, uw bekwaamheidsregistratie: per medewerker de voorbehouden en risicovolle handelingen volgens uw scholingsbeleid, met de handeling, het protocol met zijn versie, de datum, in wiens opdracht en wie de praktijktoets aftekende, actueel gehouden met wat de medewerker zelf rapporteert; vragen aan Inora tellen nooit mee; nooit de inhoud van een gesprek, een score of een gebruikscijfer	Medewerkers, met naam	Alleen het bekwaamheids-dossier dat de inspectie verwacht (Wkkgz, Wet BIG); in de pilot een voorbeeld-weergave voor het deelnemende team, tot de ondernemingsraad instemt	Europa (Ierland)	In Inora zolang de medewerker bij u werkt, plus 30 dagen; in die 30 dagen exporteert u het naar uw eigen personeels-dossier, waar uw eigen termijn geldt	Art. 6 AVG: door u in te vullen
V8	Toetsset: vragen uit uw organisatie, en antwoorden die een medewerker of een controle markeerde met hun vraag, ontdaan van namen van cliënten en medewerkers door een taalmodel in de EU; geen mens leest een vraag of antwoord eruit; alleen op uw schriftelijke opdracht, na instemming van de ondernemingsraad waar u er een heeft	Medewerkers; de cliënten over wie zij vroegen	Elke nieuwe versie van Inora toetsen voordat die in uw omgeving live gaat	Europa (Ierland)	Tot u de opdracht intrekt, uiterlijk tot het einde van de overeenkomst; daarna binnen 30 dagen weg	Art. 6 AVG; art. 9, lid 2, onder h AVG met art. 30, lid 3, onder a UAVG: door u in te vullen

Nr.	Gegevens	Van wie	Waarvoor	Waar	Hoe lang	Grondslag
V9	Antwoordverslag: per antwoord de bronnen met hun versies, de toets die het doorstond en de datum, en een kenmerk dat de medewerker bij het antwoord ziet; nooit wie vroeg, het tijdstip, de afdeling, de vraag of het antwoord	Medewerkers en cliënten, alleen voor zover herleidbaar	Verantwoorden waarop een antwoord rustte, bij een incident of een klacht	Europa (Ierland), bij Axiomatic; nooit bij de organisatie	2 jaar; daarna binnen 30 dagen uit back-ups	Art. 6 AVG: door u in te vullen
V10	Dossiergegevens, zodra Inora het dossier leest, via een koppeling of de eigen login: wat Inora uit het ECD leest voor de taak die loopt, een vraag, de voorbereiding van een bezoek, een evaluatie, een regel of signaal, ook 's nachts; geen tweede dossier	De cliënten; de medewerkers op wier naam het werk loopt	De taak uitvoeren, met de rechten van wie het werk doet	Europa (Ierland); het model in de EU, via Amazon Bedrock of Azure OpenAI	De termijn in uw verwerkersovereenkomst; wat overblijft valt onder V2	Art. 6 AVG; art. 9, lid 2, onder h AVG met art. 30, lid 3, onder a UAVG: door u in te vullen
V11	Dossierlogboek, zodra Inora het dossier leest, via een koppeling of de eigen login: per stap wat Inora deed, namens wie, voor welke cliënt en met welk resultaat; nooit wat iemand vraagt. Het ECD houdt zijn eigen logboek	Medewerkers; de cliënten over wie het gaat	Controle op dossiertoegang, ingericht volgens NEN 7513; in te zien door de functie die u aanwijst, per cliënt of bij een onderzoek, nooit als cijfer over één medewerker	Europa (Ierland)	De termijn in uw verwerkersovereenkomst	Art. 6 AVG; art. 9, lid 2, onder h AVG met art. 30, lid 3, onder a UAVG: door u in te vullen

V1 tot en met V9 volgen de volgorde en de nummers van bijlage 1 bij de verwerkersovereenkomst. De privacyverklaring telt twaalf soorten gegevens: deze elf en, als onderdeel 10, het gebruiksonderzoek, waarvoor Axiomatic zelf verwerkingsverantwoordelijke is en dat daarom niet in uw register staat; V10 en V11 zijn daar onderdeel 11 en 12. Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland).

Het bekwaamheidsdossier (V7) is het dossier van uw organisatie, dat de inspectie verwacht (Wkkgz, Wet BIG). Axiomatic houdt het in Inora bij als verwerker, op uw instructie; er is geen ander doel. Medewerkers zien hun eigen bekwaamheidsdossier in Inora en kunnen om een kopie vragen om mee te nemen: dat is hun recht op inzage (art. 15 AVG), dat uw organisatie beantwoordt en waarbij Axiomatic helpt.

Het antwoordverslag (V9) blijft bij Axiomatic en staat in geen scherm van uw organisatie. U krijgt het op schriftelijk verzoek van de functie die u in bijlage 3 aanwijst, voor een incident of een klacht, en nooit wie vroeg.

Na het einde van de overeenkomst kiest u voor teruggave of verwijdering. Tot en met dag 30 blijven de gegevens beschikbaar voor teruggave; uiterlijk op dag 30 zijn ze weg uit de actieve systemen, inclusief logboek en zoekindex; uiterlijk op dag 60 uit de back-ups. Op verzoek bevestigen wij de verwijdering schriftelijk.

2.3 Betrokkenen en ontvangers

- **Betrokkenen:** medewerkers van uw organisatie (gebruikers, auteurs en eigenaren van documenten) en cliënten over wie medewerkers een vraag stellen.
- **Ontvangers:** twee subverwerkers, beide in de EU: Amazon Web Services EMEA SARL (hosting, Amazon Bedrock) en Microsoft Ireland Operations Limited (Azure OpenAI). Niemand anders. Wij verkopen niets, delen niets met andere klanten en voegen niets samen. Alleen de anonieme aantallen uit het gebruiksonderzoek telt Axiomatic, als verwerkingsverantwoordelijke, op over ten minste vijf organisaties (privacyverklaring, punt 10).
- **Doorgifte buiten de EER:** geen. Verwerking buiten de EU vraagt eerst een schriftelijke wijziging van de verwerkersovereenkomst en een grond uit hoofdstuk V AVG.

3. Doeleinden

Inora verwerkt persoonsgegevens voor één algemeen doel: zorgmedewerkers antwoord geven uit de eigen bronnen van de organisatie en rapportages laten opstellen in haar format. De verwerkingen V3 tot en met V9 dienen dat doel: inloggen, beveiliging, ondersteuning, het beheer van uw omgeving, het bekwaamheidsdossier dat de inspectie verwacht, alleen op uw schriftelijke opdracht de toetsset waarmee wij elke nieuwe versie toetsen voordat die in uw omgeving live gaat, en het antwoordverslag dat vastlegt waarop een antwoord rustte. Elke bron van de organisatie is in het antwoord gemarkeerd, de passage staat één tik verder, en staat het antwoord niet in de bronnen, dan zegt Inora dat.

Axiomatic gebruikt de gegevens niet voor eigen doeleinden, behalve de anonieme aantallen van het gebruiksonderzoek, waarvoor Axiomatic zelf verwerkingsverantwoordelijke is (privacyverklaring, onderdeel 10). Axiomatic traint er geen model mee en laat geen subverwerker dat doen, en voegt de gegevens van uw organisatie niet samen met die van een andere; alleen de anonieme aantallen van het gebruiksonderzoek tellen wij op, over ten minste vijf organisaties. Inora stelt geen diagnose en beslist niet over een behandeling: de professional beslist. Inora ondersteunt triage en triageert nooit zelf; door zijn beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.

Uw deel. Bevestigen dat dit uw doel is, voor elk team en elke locatie waar Inora komt.

4. Grondslag, noodzaak en evenredigheid

4.1 De grondslag

De grondslag is van uw organisatie. Voor elke verwerking stelt zij een grond uit artikel 6 AVG vast. Voor gezondheidsgegevens is daarnaast een uitzondering op het verbod van artikel 9 AVG nodig: artikel 9, lid 2, onder h AVG met artikel 30, lid 3, onder a UAVG kan gelden voor noodzakelijke verwerking bij behandeling, verzorging of het beheer van de instelling. Dat geldt niet vanzelf voor elk gebruik; u beoordeelt de noodzaak en het beroepsgeheim.

Wat de wet van ons als verwerker vraagt bij gezondheidsgegevens: geheimhouding door iedereen die bij de gegevens kan. Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend, en iedereen met toegang tot productie heeft een VOG (art. 9, lid 3 AVG; art. 30, lid 4 UAVG).

4.2 Minimale gegevens

- **Alles wat getypt of ingesproken wordt, geldt als gezondheidsgegeven** en wordt zo beveiligd.
- **Geen tweede cliëntdossier.** Inora houdt geen dossier bij naast het uwe.
- **Geen BSN.** Inora vraagt nergens om een burgerservicenummer.
- **Met single sign-on geen wachtwoorden.** Inloggen loopt via uw eigen identiteitsbeheer (OpenID Connect of SAML). Met single sign-on bewaart Inora geen wachtwoorden.
- **Alleen wat uw single sign-on al kent:** naam, zakelijk e-mailadres, unieke code en groepen.
- **Korte bewaartermijn:** gesprekken standaard 90 dagen; een langere termijn weegt u in deze DPIA.

4.3 Evenredigheid en alternatieven

Het alternatief voor Inora is wat er nu gebeurt: zoeken in mappen of op het intranet, een collega bellen die het weet, of het niet weten. Die alternatieven verwerken minder gegevens, maar laten de medewerker op het moment van zorg zonder de geldende werkafspraak, of verspreiden dezelfde cliëntgegevens over telefoon en chat zonder vastlegging.

Uw deel. De grondslag vaststellen per verwerking (V1 tot en met V11), en de afweging tegen de alternatieven voor uw organisatie.

5. Risico's voor betrokkenen

Elk risico met de kans en het gevolg zonder maatregel, de maatregel en het restrisico zoals Axiomatic het inschat. Uw organisatie weegt ze voor haar eigen teams en cliënten.

Nr.	Risico	Kans	Gevolg	Maatregel	Restrisico
R1	Gezondheidsgegevens van cliënten in getypte of ingesproken tekst, gelezen door wie dat niet mag	Middel	Hoog	Alles getypt of ingesproken geldt als gezondheidsgegeven; TLS 1.2 of hoger, AES-256 in opslag; eigen omgeving per organisatie; inloggen via uw identiteitsbeheer met single sign-on, sessie eindigt uiterlijk na acht uur; geen BSN, geen tweede dossier; 90 dagen bewaard	Laag
R2	Meekijken met medewerkers: vragen of tempo gebruikt tegen een medewerker	Middel	Hoog	De vier regels van §7: geen scherm met gesprekken in de organisatie; verslagen per team van minstens vijf, het onderwerp ingedeeld door het taalmodel dat het antwoord schrijft, zonder namen; onbeantwoorde vragen als onderwerp, zonder naam en zonder de woorden van de medewerker; inzage door Axiomatic alleen op schriftelijk verzoek, voor een incident of een klacht, vastgelegd, de medewerker geïnformeerd; bij een storing alleen de logging en het antwoordverslag, nooit een gesprek. Geen score, geen beoordeling, geen emotieherkenning (AI-verordening art. 5, lid 1, onder f); inlogmomenten en IP-adressen van één medewerker nooit naar de organisatie. Dienstmetingen en het bekwaamheidsdossier: R6 en R7	Laag
R3	Een onjuist antwoord met gevolg voor de cliënt	Laag	Hoog	Elk antwoord rust op de bronnen van de organisatie, elke bron gemarkeerd, de passage één tik verder; Inora zegt het als het antwoord niet in de bronnen staat; de professional beslist	Laag
R4	Een verzoek van een buitenlandse overheid aan een Amerikaans moederbedrijf van een subverwerker	Laag	Hoog	Verwerking en opslag alleen in de EU, door AWS EMEA SARL en Microsoft Ireland Operations Limited; versleuteling; melding aan u vóór verstrekking, tenzij de wet dat verbiedt; bezwaar tegen elk verzoek zonder geldige grond; een buitenlands bevel is geen grond voor doorgifte (art. 48 AVG)	Laag, niet nul

Nr.	Risico	Kans	Gevolg	Maatregel	Restrisico
R5	Een datalek	Laag	Hoog	Ingericht volgens NEN 7510 en ISO 27001; alleen de engineers die Inora bouwen bij productie, bij naam in de verwerkersovereenkomst, met persoonlijk account, MFA en VOG, elke toegang vastgelegd; bewaking; kritieke patches binnen 72 uur; melding aan u uiterlijk 24 uur na kennisname	Laag
R6	Dienstmetingen per gebruiker gebruikt als prestatiemeting van een medewerker	Laag	Hoog	Per gebruiker 30 dagen, daarna alleen opgeteld per team van minstens vijf mensen; alleen om de omgeving te beheren; nooit per medewerker naar de organisatie	Laag
R7	Een onjuiste of ontbrekende regel in het bekwaamheids-dossier, met gevolgen voor het werk van de medewerker	Laag	Hoog	Alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht; de medewerker ziet het eigen dossier in Inora en laat een fout herstellen (art. 16 AVG); nooit een score of een gebruikscijfer	Laag
R8	Een vraag in de toetsset herleid tot een cliënt of medewerker, of langer bewaard dan nodig	Laag	Middel	Alleen op uw schriftelijke opdracht, na instemming van de onderne-mingsraad waar u er een heeft; namen verwijderd door een taalmodel; geen mens leest een vraag of antwoord uit de toetsset, de toets is geautomatiseerd; alleen om nieuwe versies te toetsen; uiterlijk tot het einde van de overeenkomst, binnen 30 dagen na intrekking weg	Laag
R9	Het antwoordverslag herleid tot wie vroeg	Laag	Middel	Geen naam, tijdstip, afdeling, vraag of antwoord; het blijft bij Axiomatic; alleen langs VWO art. 5.5 en 5.6, voor een incident of een klacht	Laag

Uw deel. De weging voor uw organisatie: welke teams, welke cliënten, welke restrisico's u aanvaardt. Of voorafgaande raadpleging nodig is, staat in §6.7. Axiomatic helpt daarbij.

6. De DPIA, kop voor kop

Artikel 35, lid 7 AVG noemt wat een DPIA ten minste bevat; lid 9 vraagt de zienswijze van betrokkenen, artikel 36 de afweging over voorafgaande raadpleging. Per kop: wat Axiomatic invulde, wat van u is en waar het onderbouwd staat. Dit dossier is het ene DPIA-document van Inora, openbaar; Axiomatic levert het kosteloos.

6.1 Systematische beschrijving (art. 35, lid 7, onder a)

Ingevuld door Axiomatic. Negen verwerkingen, twee erbij zodra Inora het dossier leest, via een koppeling of de eigen login. In de volgorde van VWO bijlage 1: documenten, vragen met antwoorden en rapportages, accounts uit uw identiteitsbeheer, het logboek, ondersteuning en implementatie, dienstmetingen, het bekwaamheidsdossier, de toetsset en het antwoordverslag. Betrokkenen: uw medewerkers en de cliënten over wie zij vragen. Ontvangers: twee subverwerkers, beide in de EU: Amazon Web Services EMEA SARL (hosting, Amazon Bedrock) en Microsoft Ireland Operations Limited (Azure OpenAI). Zie §2.

Uw deel. De omvang: hoeveel medewerkers, welke teams en locaties, hoeveel bronnen.

Staat in. Dit dossier §2; Subverwerkers versie 1.6.

6.2 Doeleinden (art. 35, lid 7, onder a)

Ingevuld door Axiomatic. Antwoord uit de eigen bronnen van de organisatie en rapportages in haar format, met per verwerking het doel uit het register, en geen ander. Geen training, nooit samengevoegd met een andere organisatie. Zie §3.

Uw deel. Bevestigen dat dit uw doel is, voor elk team waar Inora komt.

Staat in. VWO art. 3.1, 3.3 en 3.9; dit dossier §3.

6.3 Noodzaak en evenredigheid (art. 35, lid 7, onder b)

Ingevuld door Axiomatic. Geen BSN, geen tweede cliëntdossier. Met single sign-on geen wachtwoorden en alleen wat uw single sign-on al kent. Gesprekken standaard 90 dagen; een langere termijn weegt u in deze DPIA. Zie §4.

Uw deel. De grondslag vaststellen, en de afweging tegen wat er nu gebeurt: zoeken op het intranet, een collega bellen, het niet weten.

Staat in. Dit dossier §4, Grondslagen.

6.4 Risico's voor betrokkenen (art. 35, lid 7, onder c)

Ingevuld door Axiomatic. Negen risico's, elk met kans, gevolg en maatregel: gezondheidsgegevens in getypte of ingesproken tekst, meekijken met medewerkers, een onjuist antwoord, een verzoek van een buitenlandse overheid, een datalek, dienstmetingen gebruikt als prestatiemeting, een fout in het bekwaamheidsdossier, een vraag in de toetsset (alleen op uw opdracht) die herleid of te lang bewaard wordt, en het antwoordverslag herleid tot wie vroeg. Zie §5.

Uw deel. De weging voor uw organisatie: welke teams, welke cliënten, welke restrisico's u aanvaardt.

Staat in. Dit dossier §5, de risicotabel.

6.5 Maatregelen (art. 35, lid 7, onder d)

Ingevuld door Axiomatic. Ingericht volgens NEN 7510 en ISO 27001. Eigen omgeving per organisatie (eigen database, documentopslag en zoekindex), inloggen via uw identiteitsbeheer met single sign-on, TLS 1.2 of hoger en AES-256, alleen de engineers die Inora bouwen bij productie, bij naam in de verwerkersovereenkomst, met MFA en VOG, elke toegang vastgelegd, logboek 12 maanden. Back-ups dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland), met een hersteltest elk kwartaal. Melding van een datalek uiterlijk 24 uur na kennisname.

Uw deel. Uw eigen maatregelen: welke groepen toegang krijgen, wie bronnen beheert, en wat u medewerkers vraagt over wat zij typen.

Staat in. Beveiligingsoverzicht versie 1.4; de controlematrix, de basis voor uw verklaring van toepasselijkheid.

6.6 Zienswijze van betrokkenen (art. 35, lid 9)

Ingevuld door Axiomatic. Uw medewerkers spreken via de ondernemingsraad: zijn instemming (art. 27 WOR) is hun zienswijze. Het instemmingsverzoek ligt klaar, met de vier regels over gesprekken uit §7.

Uw deel. De instemming vragen en vastleggen, en zo nodig de cliëntenraad horen.

Staat in. De pagina Ondernemingsraad (axiomatic.digital/producten/beoordelen/ondernemingsraad); het instemmingsverzoek.

6.7 Voorafgaande raadpleging (art. 36)

Ingevuld door Axiomatic. Niet nodig als de maatregelen van §5 en §6.5 het hoge risico wegnemen. Onze inschatting van het restrisico staat per risico in de risicotabel van §5.

Uw deel. Uw FG weegt het restrisico en legt de afweging vast. Blijft er een hoog risico, dan raadpleegt u de Autoriteit Persoonsgegevens vóór de start.

Staat in. Dit dossier §5

7. Gesprekken van medewerkers: vier regels

Wat een medewerker aan Inora vraagt, leest niemand in de organisatie; Axiomatic alleen langs de regels hieronder. De vier regels, elk met waar ze gebonden zijn. U kunt dit hoofdstuk zo aan de ondernemingsraad geven.

1. **Niemand in de organisatie leest een gesprek mee, ook de leiding niet.** Geen beheerder, leidinggevende of bestuurder kan in Inora de vragen en antwoorden van een medewerker openen; een scherm daarvoor bestaat niet. *Gebonden in:* privacyverklaring, Gesprekken van medewerkers
2. **Verslagen gaan over teams van minstens vijf mensen.** Het maandverslag toont per team de onderwerpen waarover gevraagd wordt, met aantallen, nooit per medewerker. Per team naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams. Het onderwerp wordt tegelijk met het antwoord bepaald, zonder namen; geen mens leest mee. Inora beoordeelt niemand en geeft niemand een score. *Gebonden in:* privacyverklaring, Gesprekken van medewerkers
3. **Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg, naar wie over het onderwerp gaat**, met een aantal en per protocol, zodat de bron kan worden aangevuld. Bijvoorbeeld: *Insulinepen: houdbaarheid buiten de koelkast · 2×*. *Gebonden in:* privacyverklaring, Gesprekken van medewerkers
4. **Axiomatic leest een gesprek alleen op schriftelijk verzoek, voor een incident of een klacht.** Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die u in bijlage 3 van de VWO aanwijst, zoals uw functionaris gegevensbescherming, voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt. *Gebonden in:* privacyverklaring, Gesprekken van medewerkers

VWO art. 5.6, letterlijk: *“5.6 Verwerker verstrekt Verwerkingsverantwoordelijke geen cijfer, score of beoordeling over één medewerker en geen inhoud van diens gesprekken. Ook inlogmomenten en IP-adressen van één medewerker verstrekt Verwerker niet; de logging gaat op verzoek opgeteld per team van minstens vijf mensen en per dag, en een dag met minder dan vijf inlogs staat er als ‘<5’ (Bijlage 1, onderdeel 4). Verslagen over het gebruik gaan alleen over teams van minstens vijf mensen: per team naar de teamleider en de ondernemingsraad; het bestuur en kwaliteit ontvangen alleen de som over alle teams. Voor die verslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, zonder namen; geen mens leest mee, en de indeling blijft in de Omgeving en verdwijnt met het gesprek (Bijlage 1, onderdeel 2). Deze verslagen horen bij Inora en vragen geen aparte opdracht. Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg, naar wie over het onderwerp gaat. Een onderwerp dat één keer gevraagd werd, gaat pas mee als het een tweede keer komt; na drie maanden gaat het alleen mee in de som over alle teams. Naast wat de medewerker zelf verstuurt, zoals een rapportage na akkoord of een MIC-melding, gaat alleen het bekwaamheidsdossier dat de inspectie van Verwerkingsverantwoordelijke verwacht (Wkkgz, Wet BIG), voor voorbehouden en risicovolle handelingen volgens haar scholingsbeleid, per medewerker naar Verwerkingsverantwoordelijke. Het legt alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. Het bekwaamheidsdossier zien alleen de teamleider en de opleiding van Verwerkingsverantwoordelijke, en de medewerker zelf. De medewerker ziet het eigen bekwaamheidsdossier in Inora en krijgt op verzoek een kopie (artikel 15 AVG; artikel 7). Een verzoek van een betrokkene (artikel 15 AVG) beantwoordt Verwerker langs artikel 7, met alleen wat dat verzoek vraagt, nooit als inzage voor de leiding. Een wettelijke vordering beantwoordt Verwerker langs artikel 3.7 en 6.6, met alleen wat de vordering vraagt; ook dan legt Verwerker de inzage vast en laat hij de medewerker weten dat het gesprek is ingezien, tenzij de wet dat verbiedt. Inora leidt geen emoties of stemming van een medewerker af (AI-verordening, artikel 5, lid 1, onder f). Een onjuist antwoord is een bevinding over Inora en de bron, nooit over de medewerker die het tegenkwam. Van elk antwoord houdt Verwerker een antwoordverslag bij met*

de bronnen en hun versies, het model, de toets die het doorstond, de datum en een kenmerk dat de medewerker bij het antwoord ziet, zonder wie vroeg, het tijdstip, de afdeling of de inhoud van vraag en antwoord. Het blijft bij Verwerker; Verwerkingsverantwoordelijke krijgt het alleen langs de weg van artikel 5.5 (Bijlage 1, onderdeel 9).”

Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Dat dossier is V7 in §2.2; het antwoordverslag (V9) blijft bij Axiomatic.

8. Datalekken: wie wat doet

Moment	Wie	Wat
Uur 0	Axiomatic	Ziet een datalek, of vermoedt er een.
Binnen 24 uur	Axiomatic	Meldt het aan uw contactpersoon uit VWO bijlage 3, met de aard, de betrokkenen, de gevolgen, de maatregelen en een contactpersoon. De 24 uur zijn een maximum, geen wachttijd. Meldingen noemen de soorten gegevens en het aantal betrokkenen, nooit gegevens uit Inora.
Binnen 72 uur na onze melding	Uw organisatie	Meldt het bij de Autoriteit Persoonsgegevens als het gemeld moet worden (art. 33 AVG), en zo nodig aan de betrokkenen (art. 34 AVG). Uw 72 uur beginnen zodra wij u melden; onze 24 uur gaan eraan vooraf. Axiomatic meldt niet zelf aan de toezichthouder.
Binnen 10 werkdagen	Axiomatic	Schriftelijk verslag met oorzaak, gevolgen en maatregelen.

9. Subverwerkers

Voor een organisatie in de EU heeft Inora twee subverwerkers. Amazon Web Services EMEA SARL: hosting in Europa (Ierland) en het model via Amazon Bedrock met het EU-inferentieprofiel. Microsoft Ireland Operations Limited: Taalmodellen via Azure OpenAI in de EU-regio; het systeem kiest het model. Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek. Geen van beide traint een model op uw gegevens. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model. Azure OpenAI draait Axiomatic met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (Microsoft, Abuse monitoring).

Een nieuwe of vervangende subverwerker melden wij minstens 30 dagen vooraf per e-mail. U kunt binnen die termijn bezwaar maken; zolang het niet is opgelost, verwerkt de nieuwe subverwerker niets van u. Vinden wij geen oplossing, dan zegt u dat deel op zonder vergoeding en krijgt u terug wat u vooruitbetaalde.

10. Wat u van ons krijgt

- Dit privacydossier, met de DPIA voorgevuld: het ene DPIA-document van Inora, openbaar.
- De lijst van subverwerkers, versie 1.6.
- Het beveiligingsoverzicht versie 1.4 en de controlematrix versie 1.3, de basis voor uw verklaring van toepasselijkheid.
- De privacyverklaring, op axiomatic.digital/vertrouwen/privacy.

Onze functionaris gegevensbescherming is een externe FG, bereikbaar via fg@axiomatic.digital en aangemeld bij de Autoriteit Persoonsgegevens. Vragen over dit dossier: privacy@axiomatic.digital.

AXIOMATIC

Dossier voor de ondernemingsraad

Inora en gegevens over medewerkers. Wat naar de organisatie gaat, wat nooit, en waar het staat.

Versie 1.9, 11 november 2026

Dit dossier is voor de leden en de secretaris van de ondernemingsraad van een zorgorganisatie die Inora wil invoeren. Het beantwoordt één vraag: blijven de gesprekken van onze medewerkers privé? Ja, de gesprekken van uw medewerkers blijven privé. Hieronder staat hoe, wat wel naar de organisatie gaat, en in welk document elke regel staat, zodat de raad instemt op voorwaarden en niet op beloftes.

Het instemmingsverzoek zelf, met de informatiebrief, staat in een eigen document: *Informatiebrief en model voor het instemmingsverzoek*, versie 1.7 van 7 november 2026.

1. Wat Inora is

Inora is het kennissysteem van de zorgorganisatie, gebouwd op haar eigen kennis. De zorgmedewerker stelt een vraag in gewone taal en krijgt antwoord uit de eigen protocollen, werkafspraken en richtlijnen van de organisatie, met de bron erbij. Inora maakt de rapportage klaar in het format van de organisatie; de zorgmedewerker leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft. De professional controleert en beslist.

Daarmee verdwijnen drie stappen uit de dienst: opzoeken hoe het hier moet, doen en vastleggen, en uitschrijven.

Inora is gemaakt door Axiomatic B.V. in Delft en ingericht volgens NEN 7510 en ISO 27001. Gegevens blijven in de EU of op de eigen servers van de organisatie; geen model wordt erop getraind. Medewerkers loggen in met het eigen account van hun organisatie, via single sign-on.

2. Waarom de raad instemmingsrecht heeft

Artikel 27, lid 1 WOR geeft de ondernemingsraad instemmingsrecht over:

- **onder k:** een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen;
- **onder l:** een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen.

Inora verwerkt gegevens van medewerkers en legt werk vast. Beide onderdelen zijn dus van toepassing. De bestuurder legt het besluit schriftelijk voor, met de beweegredenen en de gevolgen voor medewerkers; de raad besluit pas na minstens één overlegvergadering en laat zijn besluit schriftelijk en met redenen weten (artikel 27, lid 2). Een besluit zonder instemming is nietig als de raad daar schriftelijk een beroep op doet, binnen een maand nadat de bestuurder heeft meegedeeld dat hij het uitvoert, of nadat het de raad is gebleken (artikel 27, lid 5).

Bron: Wet op de ondernemingsraden, artikel 27.

3. De lijn

Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Die lijn is geen instelling; zij zit in Inora, en geen beheerder, leidinggevende of bestuurder zet haar anders.

	Wat Inora over het werk van een medewerker weet	Wat de lijn ermee doet
Regel 1	Gesprekken van de medewerker	Stopt. Niemand in de organisatie opent deze gesprekken, ook de leiding niet.
Regel 2	Hoe vaak, hoe snel en wanneer de medewerker werkt	Stopt. Geen cijfer over één medewerker, voor niemand in de organisatie.
Regel 3	Een oordeel over het werk van de medewerker	Stopt. Inora beoordeelt niemand en geeft niemand een score.

	Wat Inora over het werk van een medewerker weet	Wat de lijn ermee doet
Regel 4	Stemming van de medewerker	Stopt. Inora leidt geen emoties af, niet uit stem en niet uit gezicht.
Regel 5	Wat Axiomatic op verzoek inziet	Stopt. Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die de organisatie aanwijst, voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligings-incident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.
Regel 6	Waarover het team van de medewerker vraagt	Gaat door, per team van vijf of meer: het maandverslag, zonder één naam. Per team naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams.
Regel 7	Een vraag zonder antwoord	Gaat door. Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van de medewerker, naar de eigenaar, gebundeld per protocol, zodat de bron wordt aangevuld.
Regel 8	Een fout antwoord	Gaat door, als bevinding over Inora en de bron, nooit over wie het tegenkwam.
Regel 9	Een voorbehouden of risicovolle handeling	Gaat door, met naam: het bekwaamheidsdossier, met de handeling, het protocol met zijn versie, de datum en in wiens opdracht. De medewerker ziet het zelf in Inora.

Buiten de lijn, want de organisatie zet haar zelf aan en alleen als de raad ermee instemt (voorwaarde 11):

- **Toetsset.** Vragen uit de organisatie en gemarkeerde antwoorden met hun vraag, zonder namen, om elke nieuwe versie van Inora te toetsen; geen mens leest daarvoor een vraag of antwoord. Alleen op schriftelijke opdracht van de organisatie, na instemming van de ondernemingsraad.

4. Wat de leiding ziet: het maandverslag per team

Per team naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams. Het onderwerp wordt tegelijk met het antwoord bepaald, zonder namen; geen mens leest mee. Het maandverslag bevat per team van minstens vijf mensen:

- waarover gevraagd werd, per onderwerp, met het aantal vragen van het team samen;
- welke onderwerpen nog geen antwoord kregen, met een aantal, zoals hun eigenaar ze krijgt: herschreven zonder herkenbare details, zonder naam en zonder de woorden van wie vroeg, gebundeld per protocol. Een onderwerp dat één keer gevraagd werd, gaat pas mee als het een tweede keer komt; na drie maanden gaat het alleen mee in de som over alle teams;
- welke gaten in de werkafspraken gedicht zijn;
- hoeveel tijd Inora het team teruggaf.

Het bevat nooit: een naam, een vraag zoals iemand haar typte, een cijfer per persoon, tijden of tempo van één medewerker, een score. Een team van minder dan vijf mensen krijgt geen eigen verslag, zodat niemand erin te herkennen is.

Voorbeeld, Zorggroep Voorbeeld, Wijkteam Heuvelland-Oost (11 medewerkers), oktober 2026

Onderdeel	Inhoud
Waarover gevraagd werd	Wondzorg 41, Medicatie 33, Rapporteren 28, Katheterzorg 17, Overige onderwerpen 24 (143 vragen)
Nog zonder antwoord	4: Insulinepen: houdbaarheid buiten de koelkast · 2× (naar medicatiebeleid); Blaaskatheter vervangen: wie mag het · 2× (naar voorbehouden handelingen). Zonder naam en zonder de woorden van wie vroeg
Gaten gedicht	2 werkafspraken aangevuld
Tijd teruggegeven	14 uur, voor het hele team
Nachtdienst Heuvelland (4 medewerkers)	Geen eigen verslag

De cijfers zijn die van het voorbeeld; het echte verslag van een organisatie is vertrouwelijk.

5. Het bekwaamheidsdossier

Wie in opdracht van een zelfstandig bevoegde, zoals een arts, een voorbehouden handeling doet, moet daarvoor bekwaam zijn en volgt diens aanwijzingen (Wet BIG, artikel 35 en 38). Insuline subcutaan toedienen en een katheter inbrengen zijn zulke handelingen. De inspectie verwacht dat de organisatie die bekwaamheid laat zien, ook voor risicovolle handelingen. Dat bijhouden gebeurt nu vaak op papier of in een scholingssysteem, en vaak achteraf.

Dat bekwaamheidsdossier, naast wat de medewerker zelf verstuurt het enige met naam dat naar de organisatie gaat (hoofdstuk 3), gaat over voorbehouden en risicovolle handelingen volgens het scholingsbeleid van de organisatie. Het is het dossier van de organisatie zelf; Axiomatic bewaart het in Inora als verwerker, op haar instructie. Inora legt het vast uit wat de medewerker deed; vragen of gelezen informatie gaan niet mee. Het legt alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. Inora Matrix is daarvoor de bekwaamheidsregistratie van de organisatie: per functie staat erin welke handelingen het scholingsbeleid vraagt, de beoordelaar tekent de praktijktoets af in dezelfde rapportagestroom, en daarna blijft de registratie actueel met de handelingen die de medewerker zelf rapporteert, met het protocol en de versie die gold. Vragen van de medewerker aan Inora tellen nooit mee, ook niet als bewijs van bekwaamheid. In de pilot is het een voorbeeldweergave voor het deelnemende team en doen medewerkers vrijwillig mee; het officiële register wordt het pas na instemming van de ondernemingsraad.

Een voorbeeld.

Veld	Inhoud
Medewerker	Sanne de Wit, verzorgende IG
Handeling	Insuline subcutaan toedienen, voorbehouden handeling
Protocol	Insuline toedienen, versie 6
Datum	14 oktober 2026
In wiens opdracht	De behandelend arts van de cliënt

Gaat naar de organisatie	Gaat er nooit heen
Wie, welke handeling en welk protocol, met de versie	Wat zij vroeg of las
De datum, en in wiens opdracht	Hoe vaak zij Inora gebruikt
	Hoe lang zij erover deed

Gaat naar de organisatie	Gaat er nooit heen
	Een score of een oordeel

Bewaren. In Inora zolang de medewerker bij de organisatie werkt, plus 30 dagen; in die 30 dagen exporteert de organisatie het naar haar eigen personeelsdossier, waar haar eigen termijn geldt.

Wie het ziet. De medewerker zelf: het eigen bekwaamheidsdossier, altijd, in Inora. De medewerker kan om een kopie vragen om mee te nemen: dat is het recht op inzage (artikel 15 AVG), dat de organisatie beantwoordt en waarbij Axiomatic helpt. De teamleider en de opleiding: het bekwaamheidsdossier, om te weten wie welke handeling mag doen; dat moesten zij al weten. Niemand anders.

Waarom het de medewerker dient. De bekwaamheid van de medewerker staat vast op het moment zelf, niet achteraf, met het protocol en de versie die gold, en is zelf in te zien. Een bewijs van het vak, geen meetlat.

Bron: Wet BIG, artikel 35 en 38.

6. De regels op papier

Elke regel van de lijn staat letterlijk in een document dat de raad in zijn besluit kan aanhalen. De verwerkersovereenkomst ontvangt de bestuurder bij het voorstel van Axiomatic; de raad vraagt die bij de bestuurder op.

Regel 1. Niemand in de organisatie leest het gesprek van een medewerker.

- Verwerkersovereenkomst, artikel 5.5: “Geen beheerder, leidinggevende of bestuurder van Verwerkingsverantwoordelijke kan in Inora de gesprekken van een medewerker openen.”
- Privacyverklaring, Gesprekken van medewerkers: “Niemand in de organisatie leest een gesprek mee, ook de leiding niet.”

Regel 2. Niemand in de organisatie krijgt een cijfer over één medewerker.

- Inora en de AI-verordening, Wat Inora nooit doet: “Cijfers over gebruik gaan alleen over teams van minstens vijf mensen, nooit over één medewerker, en niemand krijgt een score.”

- Verwerkersovereenkomst, artikel 3.4: “Verwerkingsverantwoordelijke geeft Verwerker de instructie Dienstmetingen uitsluitend te gebruiken om haar Omgeving te beheren en problemen daarin te verhelpen.”
- Verwerkersovereenkomst, artikel 5.6: “Verwerker verstrekt Verwerkingsverantwoordelijke geen cijfer, score of beoordeling over één medewerker en geen inhoud van diens gesprekken.”

Regel 3. Inora beoordeelt niemand.

- Inora en de AI-verordening, Wat Inora nooit doet: “Het beoordeelt geen medewerkers en neemt geen besluiten over hun werk.”
- Privacyverklaring, Gesprekken van medewerkers: “Inora beoordeelt niemand en geeft niemand een score.”

Regel 4. Geen emotieherkenning.

- Verwerkersovereenkomst, artikel 5.6: “Inora leidt geen emoties of stemming van een medewerker af (AI-verordening, artikel 5, lid 1, onder f).”
- Inora en de AI-verordening, Wat Inora nooit doet: “Het leidt geen emoties of stemming van medewerkers af, niet uit stem en niet uit gezicht. Dat verbiedt artikel 5, lid 1, onder f.”

Regel 5. Axiomatic leest een gesprek alleen op schriftelijk verzoek, voor een incident of een klacht, en nooit bij een storing; de aanvrager krijgt een bevinding over Inora, nooit wat de medewerker vroeg. Van een wettelijke vordering hoort de medewerker, tenzij de wet dat verbiedt.

- Verwerkersovereenkomst, artikel 5.5: “Het gesprek van een medewerker van Verwerkingsverantwoordelijke met Inora leest Verwerker alleen in op schriftelijk verzoek van de functie die Verwerkingsverantwoordelijke daarvoor in Bijlage 3 aanwijst, zoals de functionaris gegevensbescherming, en voor het doel dat het verzoek noemt: een incident of een klacht. Verwerker leest alleen wat voor dat doel nodig is, legt elke inzage vast en laat de medewerker weten dat het gesprek is ingezien. Bij een storing of een beveiligingsincident onderzoekt Verwerker de systeemlogging en het antwoordverslag, met de bronnen, hun versies en de toetsen, en nooit een gesprek.”
- Verwerkersovereenkomst, artikel 5.6: “Een wettelijke vordering beantwoordt Verwerker langs artikel 3.7 en 6.6, met alleen wat de vordering vraagt; ook dan legt Verwerker de inzage vast en laat hij de medewerker weten dat het gesprek is ingezien, tenzij de wet dat verbiedt.”
- Privacyverklaring, Gesprekken van medewerkers: “Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las.”

Regel 6. Verslagen alleen per team van vijf of meer.

- Verwerkersovereenkomst, artikel 5.6: “Verslagen over het gebruik gaan alleen over teams van minstens vijf mensen: per team naar de teamleider en de ondernemingsraad; het bestuur en kwaliteit ontvangen alleen de som over alle teams. Voor die verslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, zonder namen; geen mens leest mee, en de indeling blijft in de Omgeving en verdwijnt met het gesprek (Bijlage 1, onderdeel 2). Deze verslagen horen bij Inora en vragen geen aparte opdracht.”
- Privacyverklaring, Gesprekken van medewerkers: “Het maandverslag toont per team de onderwerpen waarover gevraagd wordt en de onderwerpen die nog geen antwoord kregen, met een aantal, nooit een vraag zoals iemand haar typte en nooit per medewerker.”

Regel 7. Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van de medewerker, naar de eigenaar.

- Verwerkersovereenkomst, artikel 5.6: “Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg, naar wie over het onderwerp gaat. Een onderwerp dat één keer gevraagd werd, gaat pas mee als het een tweede keer komt; na drie maanden gaat het alleen mee in de som over alle teams.”
- Privacyverklaring, Gesprekken van medewerkers: “Staat het antwoord niet in de bronnen, dan krijgt wie over het onderwerp gaat het onderwerp, herschreven zonder herkenbare details en zonder de woorden van wie vroeg, met het aantal keer dat het gevraagd werd, per protocol en opgeteld over alle teams, zodat de bron kan worden aangevuld. De naam van wie vroeg, gaat niet mee.”

Regel 8. Een fout is een bevinding over het systeem.

- Verwerkersovereenkomst, artikel 5.6: “Een onjuist antwoord is een bevinding over Inora en de bron, nooit over de medewerker die het tegenkwam.”
- Vertrouwen, Niemand krijgt de schuld: “Zonder schuldvraag: in de bron, het model, de software eromheen, de inrichting en onze eigen werkwijze. Geen bevinding noemt wie de fout tegenkwam.”
- Instemmingsverzoek, voorwaarde 8: “Een onjuist antwoord is een bevinding over Inora en de bron, nooit over de medewerker die het tegenkwam.”

Regel 9. Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie; met naam gaat alleen het bekwaamheidsdossier.

- Dossierlogboek: het dossierlogboek toont, zodra Inora het dossier leest, via een koppeling of de eigen login, per stap wat Inora deed en namens wie. De functie die de organisatie aanwijst, ziet het alleen op schriftelijk verzoek, per cliënt of bij een onderzoek, ter controle op dossiertoegang; het is geen cijfer over een medewerker en bevat nooit wat iemand vraagt.
- Verwerkersovereenkomst, artikel 5.6: “Naast wat de medewerker zelf verstuurt, zoals een rapportage na akkoord of een MIC-melding, gaat alleen het bekwaamheidsdossier dat de inspectie van Verwerkingsverantwoordelijke verwacht (Wkkgz, Wet BIG), voor voorbehouden en risicovolle handelingen volgens haar scholingsbeleid, per medewerker naar Verwerkingsverantwoordelijke. Het legt alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. Het bekwaamheidsdossier zien alleen de teamleider en de opleiding van Verwerkingsverantwoordelijke, en de medewerker zelf. De medewerker ziet het eigen bekwaamheidsdossier in Inora en krijgt op verzoek een kopie (artikel 15 AVG; artikel 7).”
- Privacyverklaring, Gesprekken van medewerkers: “Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Dat dossier gaat over voorbehouden en risicovolle handelingen volgens het scholingsbeleid van de organisatie, en het is het dossier van de organisatie zelf.”
- Instemmingsverzoek, voorwaarde 9: “Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Vragen van de zorgmedewerker aan Inora tellen nooit mee, ook niet als bewijs van bekwaamheid.”

De toetsset: alleen met instemming van de raad.

- Verwerkersovereenkomst, artikel 3.8: “Geen Medewerker van Verwerker leest een vraag of antwoord uit de toetsset; de toets van een nieuwe versie is geautomatiseerd.”
- Instemmingsverzoek, voorwaarde 11: “De toetsset zetten wij alleen aan als u daarmee hieronder apart instemt.”

7. Bewaren en loggen

Gegeven	Waarvoor	Hoe lang, en wat de organisatie ervan krijgt
Documenten: namen en functies van medewerkers als auteur of eigenaar	Als bron tonen	Zolang het document in Inora staat
Account: naam, zakelijk e-mailadres, unieke code en groepen	Zodat alleen bevoegde medewerkers toegang hebben	Zolang de medewerker toegang heeft, en 30 dagen daarna
Gesprekken: vragen, antwoorden en opgestelde rapportages, en het onderwerp van elk gesprek, zonder namen	Zodat de medewerker het eigen gesprek terugvindt, en het onderwerp voor het maandverslag per team	Standaard 90 dagen, door de organisatie in te stellen; niemand in de organisatie opent ze. Vraagt de organisatie binnen de bewaartermijn dat Axiomatic een gesprek inziet voor een incident of een klacht, dan houdt Axiomatic het vast tot het onderzoek klaar is en verwijdert het daarna binnen 30 dagen; de medewerker hoort ervan
Logging: inlogmomenten, beheerhandelingen en elke toegang door Axiomatic	De dienst veilig houden	12 maanden. Op verzoek krijgt de organisatie de logging alleen opgeteld per team van minstens vijf mensen en per dag; een dag met minder dan vijf inlogs staat er als ‘<5’; inlogmomenten en IP-adressen van één medewerker nooit
Dienstmetingen: aantallen vragen en responstijden per gebruiker	Alleen om de omgeving te beheren	Per gebruiker 30 dagen, daarna alleen opgeteld per team van minstens vijf mensen; nooit per medewerker naar de organisatie
Toetsset: vragen uit de organisatie en gemarkeerde antwoorden met hun vraag, namen verwijderd	Alleen op schriftelijke opdracht van de organisatie, na instemming van de ondernemingsraad, om nieuwe versies te toetsen; geen mens leest daarvoor een vraag of antwoord	Tot de organisatie de opdracht intrekt, uiterlijk tot het einde van de overeenkomst; daarna binnen 30 dagen weg

Gegeven	Waarvoor	Hoe lang, en wat de organisatie ervan krijgt
Bekwaamheidsdossier: de handeling, het protocol met zijn versie, de datum en in wiens opdracht	Het dossier dat de inspectie van de organisatie verwacht (Wkkgz, Wet BIG)	In Inora zolang de medewerker bij de organisatie werkt, plus 30 dagen; in die 30 dagen exporteert de organisatie het naar haar eigen personeelsdossier, waar haar eigen termijn geldt
Antwoordverslag: per antwoord de bronnen met hun versies, de toets die het doorstond en de datum, en een kenmerk dat de medewerker bij het antwoord ziet; nooit wie vroeg, het tijdstip, de afdeling, de vraag of het antwoord	Verantwoorden waarop een antwoord rustte, bij een incident of een klacht	2 jaar, bij Axiomatic. De organisatie krijgt het alleen op schriftelijk verzoek, nooit wie vroeg

Behalve het bekwaamheidsdossier en wat de medewerker zelf verstuurt, gaat van geen van deze gegevens iets per medewerker naar de organisatie. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek, en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen. Na het einde van de overeenkomst is alles binnen 30 dagen uit de actieve systemen en binnen 60 dagen uit de back-ups verwijderd, en op verzoek schriftelijk bevestigd.

8. Wat medewerkers winnen

De raad beschermt medewerkers, en weegt ook wat zij krijgen. Inora haalt drie stappen uit de dienst: opzoeken hoe het hier moet (het eigen protocol, met de bron, aan het bed), doen en vastleggen, en uitschrijven (het verslag staat klaar voor de zorgmedewerker weer instapt: Inora maakt het klaar, de zorgmedewerker tekent, en na akkoord gaat het dossier in). Zorgmedewerkers zeggen het zelf:

- “Fijn om even iets te checken zonder iemand te hoeven bellen. Geeft zekerheid.” Zorgmedewerker, Zuid-Limburg, vragenlijstrapportage ZorgConnect Zuid-Limburg, 12 januari 2026.
- “Het helpt me om gesprekken met artsen, cliënten of familie beter te voeren en me veiliger te voelen in mijn werk, ook als er geen collega in de buurt is om een vraag te stellen.” Verpleegkundige, Limburg, De Limburger, 22 april 2026.

- “Het bevestigt wat ik al weet, dat geeft rust.” Zorgmedewerker, Zuid-Limburg, vragenlijstrapportage ZorgConnect Zuid-Limburg, 12 januari 2026.

De tijd die terugkomt. Die gaat terug naar de zorg: naar cliënten, en naar het werk dat nu na de dienst blijft liggen. Over de formatie beslist de organisatie, niet Axiomatic, en Axiomatic verkoopt Inora nooit als bezuiniging op mensen. Het modelverzoek legt dat vast als voorwaarde 10. Een subsidieaanvraag rekent in bespaarde fte, zoals de regeling vraagt; wat de organisatie met die tijd doet, legt de bestuurder de raad apart voor.

Ondernemingsraden van zorgorganisaties die met Inora werken, stemden in op een verzoek met dezelfde regels, meestal in één vergadering. “We hebben in één vergadering ingestemd. De brief lag er al.” OR-lid, zorggroep.

9. Instemmen, evalueren en wijzigen

Het model voor het instemmingsverzoek legt de negen regels van de lijn vast als voorwaarden van de instemming, met de afspraak over de tijd die terugkomt als tiende en de toetsset als elfde: die zet de organisatie alleen aan als de raad ermee instemt. Daarnaast:

- **Wanneer.** De bestuurder legt het instemmingsverzoek tijdens de pilot aan u voor: in een apotheek de apotheekhouder, in een gemeente de directie. De raad stemt in na minstens één overlegvergadering (artikel 27, lid 2 WOR); zonder instemming volgen geen andere teams en wordt Inora Matrix niet het officiële bekwaamheidsregister. De pilot duurt acht weken; daarna besluit de organisatie welke teams volgen, en elk nieuw doel legt zij als nieuw instemmingsverzoek aan u voor.
- **Evalueren.** De bestuurder evalueert de invoering met de raad na de pilot van acht weken en daarna elk jaar, met het maandverslag per team en een overzicht van elke inzage door Axiomatic, zonder de inhoud ervan.
- **Wijzigen.** Elke wijziging van de voorwaarden, en elk ander doel, komt als nieuw verzoek om instemming terug bij de raad. Wat de leiding per team ziet, kan niet stilletjes ruimer worden; de afspraken met Axiomatic veranderen alleen schriftelijk.
- **Als een voorwaarde niet wordt nageleefd.** Gebruik buiten de voorwaarden is een besluit zonder instemming. De raad kan schriftelijk een beroep doen op de nietigheid, binnen een maand nadat de bestuurder dat gebruik heeft meegedeeld of nadat het de raad is gebleken (artikel 27, lid 5 WOR), en de bestuurder stopt dat gebruik.

10. De documenten bij dit dossier

- Privacyverklaring, met Gesprekken van medewerkers: axiomatic.digital/vertrouwen/privacy.
- Inora en de AI-verordening, met Wat Inora nooit doet: axiomatic.digital/vertrouwen/ai-act.
- Verwerkersovereenkomst met Axiomatic.
- Een voorbeeld van het maandverslag per team (paragraaf 4).
- Informatiebrief en model voor het instemmingsverzoek, versie 1.7 van 7 november 2026.

AXIOMATIC

Informatiebrief en model voor het instemmingsverzoek

Inora, voor de ondernemingsraad. Artikel 27, lid 1, onder k en l WOR.

Versie 1.7, 7 november 2026

Dit document bevat twee stukken, elk op een nieuwe pagina:

1. **De informatiebrief aan de ondernemingsraad**: wat Inora is, welke regels voor gegevens over medewerkers in het systeem zitten en welke bepalingen ze binden.
2. **Het model voor het instemmingsverzoek**: het voorgenomen besluit dat de bestuurder de ondernemingsraad schriftelijk voorlegt (artikel 27, lid 2 WOR), met de voorwaarden waaronder de raad instemt vóór de uitrol naar meer teams na de pilot en vóórdat Inora Matrix het officiële bekwaamheidsregister wordt.

Vul de tekst tussen vierkante haken in. Pas aan wat in uw organisatie anders is; de voorwaarden in artikel 4 van het verzoek laat u staan, want daarop rust de instemming.

1. De informatiebrief

[Naam van de organisatie]
Aan de ondernemingsraad
[Plaats], [datum]

Onderwerp: informatie bij het verzoek om instemming met de invoering van Inora

Geachte leden van de ondernemingsraad,

Wij vragen u binnenkort om instemming met de invoering van Inora. Voordat u daarover besluit, krijgt u in deze brief alles wat u nodig hebt: wat Inora is, wat het met gegevens over medewerkers doet en niet doet, en in welk document elke regel staat. U hoeft niets op ons woord aan te nemen.

Wat Inora is

Inora is het kennissysteem van onze organisatie, gebouwd op onze eigen kennis. Een medewerker stelt een vraag in gewone taal, aan het bed of in de auto, en krijgt antwoord uit onze eigen protocollen, werkafspraken en richtlijnen, met de bron erbij. Inora maakt de rapportage klaar in ons eigen format; de medewerker leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft. De medewerker controleert het antwoord aan de bron en beslist zelf.

Daarmee verdwijnen drie stappen uit de dienst: opzoeken hoe het bij ons moet, doen en vastleggen, en uitschrijven. Dat werk gebeurt nu vaak na de dienst.

Inora is gemaakt door Axiomatic B.V. in Delft. Het is ingericht volgens NEN 7510 en ISO 27001. Gegevens blijven in de Europese Unie, of op onze eigen servers, en geen model wordt erop getraind. Medewerkers loggen in met hun eigen account van onze organisatie.

Waarom u instemmingsrecht hebt

Inora verwerkt gegevens van medewerkers: hun account, hun vragen en de antwoorden die zij kregen. Een regeling over het verwerken en beschermen van persoonsgegevens van medewerkers (artikel 27, lid 1, onder k WOR) en een regeling over voorzieningen die geschikt zijn om de aanwezigheid, het gedrag of de prestaties van medewerkers waar te nemen of te controleren (onder l) vragen uw instemming. Dat geldt voor elk systeem dat gegevens over werk vastlegt, ook als het niet bedoeld is om mee te kijken. U hebt gelijk dat u erom vraagt.

De lijn: wat over een medewerker naar de organisatie gaat, en wat nooit

Inora is gebouwd rond één regel: niets over een individuele medewerker gaat naar de organisatie, behalve wat de medewerker zelf verstuurt en het bekwaamheidsdossier. Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Die lijn is geen instelling die een beheerder kan veranderen; zij zit in het systeem.

Wat nooit naar de organisatie gaat

- **Wat de medewerker vraagt en leest.** Niemand in de organisatie leest een gesprek mee, ook de leiding niet. Geen beheerder, leidinggevende of bestuurder kan de vragen en antwoorden van een medewerker openen.

- **Hoe vaak, hoe snel en wanneer de medewerker werkt.** Niemand in de organisatie krijgt een cijfer over één medewerker. Cijfers over gebruik gaan alleen over teams van minstens vijf mensen.
- **Een oordeel over het werk van de medewerker.** Inora beoordeelt niemand en geeft niemand een score.
- **De stemming van de medewerker.** Inora leidt geen emoties of stemming af, niet uit stem en niet uit gezicht. De AI-verordening verbiedt dat (artikel 5, lid 1, onder f).
- **Wat Axiomatic op verzoek inziet.** Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die wij daarvoor aanwijzen, zoals de functionaris gegevensbescherming, voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.

Wat wel naar de organisatie gaat, en waarom dat medewerkers beschermt

- **Het maandverslag per team.** Per team van minstens vijf mensen: waarover gevraagd werd, welke onderwerpen nog geen antwoord kregen, met een aantal, welke gaten in de werkafspraken gedicht zijn en hoeveel tijd Inora het team teruggaf. Geen naam, geen vraag zoals iemand haar typte, geen cijfer per persoon, geen score. Het onderwerp wordt tegelijk met het antwoord bepaald, zonder namen; geen mens leest mee. Per team naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams. Een team van minder dan vijf krijgt geen eigen verslag.
- **Een vraag zonder antwoord, als onderwerp.** Staat het antwoord niet in onze bronnen, dan krijgt wie over het onderwerp gaat het onderwerp, herschreven zonder herkenbare details en zonder de woorden van wie vroeg, met het aantal keer dat het gevraagd werd, gebundeld per protocol en opgeteld over alle teams, zodat de bron wordt aangevuld. De naam van wie vroeg, gaat niet mee. Een onderwerp dat één keer gevraagd werd, gaat pas mee als het een tweede keer komt; na drie maanden gaat het alleen mee in de som over alle teams.
- **Een fout antwoord, als bevinding over het systeem.** Komt een medewerker een onjuist antwoord tegen, dan is dat een bevinding over Inora en de bron. Geen bevinding noemt wie de fout tegenkwam.

- **Het bekwaamheidsdossier.** Wie in opdracht van een zelfstandig bevoegde, zoals een arts, een voorbehouden handeling doet, moet daarvoor bekwaam zijn en volgt diens aanwijzingen (Wet BIG, artikel 35 en 38), en de inspectie verwacht dat wij die bekwaamheid laten zien, ook voor risicovolle handelingen. Inora Matrix is daarvoor onze bekwaamheidsregistratie: per functie staat erin welke handelingen ons scholingsbeleid vraagt, de beoordelaar tekent de praktijktoets af, en daarna blijft het dossier actueel met de handelingen die de medewerker zelf rapporteert, met het bijbehorende protocol en de geldende versie. Vragen van de medewerker aan Inora tellen nooit mee, ook niet als bewijs van bekwaamheid. Het is ons eigen dossier; Axiomatic bewaart het in Inora als verwerker. Het legt alleen de handeling, het protocol met zijn versie, de datum, in wiens opdracht en wie de praktijktoets aftekende vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. In de pilot is het een voorbeeldweergave voor het deelnemende team en doen medewerkers vrijwillig mee; ons officiële register wordt het pas na uw instemming. Het bekwaamheidsdossier zien bij ons alleen de teamleider en de opleiding, en de medewerker zelf. De medewerker ziet het eigen bekwaamheidsdossier in Inora en krijgt op verzoek een kopie (artikel 15 AVG).

Wat wordt bewaard, en hoe lang

Gegeven	Waarvoor	Hoe lang, en wat wij ervan krijgen
Documenten: namen en functies van medewerkers als auteur of eigenaar	Als bron tonen	Zolang het document in Inora staat
Account: naam, zakelijk e-mailadres, unieke code en groepen uit ons identiteitsbeheer	Zodat alleen bevoegde medewerkers toegang hebben	Zolang de medewerker toegang heeft, en 30 dagen daarna
Gesprekken: vragen, antwoorden en opgestelde rapportages, en het onderwerp van elk gesprek, zonder namen	Zodat de medewerker het eigen gesprek terugvindt, en het onderwerp voor het maandverslag per team	Standaard 90 dagen; wij stellen de termijn in. Niemand in onze organisatie opent ze. Vragen wij binnen de bewaartermijn dat Axiomatic een gesprek inziet voor een incident of een klacht, dan houdt Axiomatic het vast tot het onderzoek klaar is en verwijdert het daarna binnen 30 dagen; de medewerker hoort ervan

Gegeven	Waarvoor	Hoe lang, en wat wij ervan krijgen
Logging: inlogmomenten, beheerhandelingen en elke toegang door Axiomatic	De dienst veilig houden	12 maanden. Op verzoek krijgen wij de logging alleen opgeteld per team van minstens vijf mensen en per dag; een dag met minder dan vijf inlogs staat er als ‘<5’; inlogmomenten en IP-adressen van één medewerker nooit
Dienstmetingen: aantallen vragen en responstijden per gebruiker	Alleen om de omgeving te beheren	Per gebruiker 30 dagen, daarna alleen opgeteld per team van minstens vijf mensen; nooit per medewerker naar ons
Toetsset: vragen uit onze organisatie en gemarkeerde antwoorden met hun vraag, zonder namen	Alleen op onze schriftelijke opdracht, na uw instemming, om nieuwe versies te toetsen; geen mens leest daarvoor een vraag of antwoord	Tot wij de opdracht intrekken, uiterlijk tot het einde van de overeenkomst; daarna binnen 30 dagen weg
Bekwaamheidsdossier: de handeling, het protocol met zijn versie, de datum, in wiens opdracht en wie de praktijktoets aftekende; nooit de inhoud van een gesprek, een score of een gebruikscijfer	Het dossier dat de inspectie van ons verwacht (Wkkgz, Wet BIG)	In Inora zolang de medewerker bij ons werkt, plus 30 dagen; in die 30 dagen exporteren wij het naar ons eigen personeelsdossier, waar onze eigen termijn geldt
Antwoordverslag: per antwoord de bronnen met hun versies, de toets die het doorstond en de datum, en een kenmerk dat de medewerker bij het antwoord ziet; nooit wie vroeg, het tijdstip, de afdeling, de vraag of het antwoord	Verantwoorden waarop een antwoord rustte, bij een incident of een klacht	2 jaar, bij Axiomatic. Wij krijgen het alleen op schriftelijk verzoek, nooit wie vroeg

Behalve het bekwaamheidsdossier en wat de medewerker zelf verstuurt, krijgen wij van geen van deze gegevens iets per medewerker. Na het einde van de overeenkomst is alles binnen 30 dagen uit de actieve systemen verwijderd en binnen 60 dagen uit de back-ups, en op verzoek bevestigt Axiomatic dat schriftelijk.

Waar elke regel staat

Regel	Waar hij staat
Niemand in de organisatie leest een gesprek	Verwerkersovereenkomst, art. 5.5; Privacyverklaring, Gesprekken van medewerkers
Niemand in de organisatie krijgt een cijfer over één medewerker	Inora en de AI-verordening, Wat Inora nooit doet.6
Niemand krijgt een score	Inora en de AI-verordening, Wat Inora nooit doet; Privacyverklaring, Gesprekken van medewerkers
Geen emotieherkenning	Verwerkersovereenkomst, art. 5.6; Inora en de AI-verordening, Wat Inora nooit doet; AI-verordening, art. 5, lid 1, onder f
Axiomatic leest een gesprek alleen op schriftelijk verzoek, nooit bij een storing; van een wettelijke vordering hoort de medewerker	Verwerkersovereenkomst, art. 5.4, 5.5 en 5.6; Privacyverklaring, Gesprekken van medewerkers
Verslagen alleen per team van vijf of meer, per team naar de teamleider en de ondernemingsraad	Verwerkersovereenkomst, art. 5.6; Privacyverklaring, Gesprekken van medewerkers
Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg	Verwerkersovereenkomst, art. 5.6; Privacyverklaring, Gesprekken van medewerkers
Een fout is een bevinding over het systeem	Verwerkersovereenkomst, art. 5.6; Vertrouwen, Als het fout gaat; dit verzoek, voorwaarde 8
Wat een medewerker vraagt, komt nooit bij de organisatie; met naam alleen het bekwaamheidsdossier	Verwerkersovereenkomst, art. 5.6; Privacyverklaring, Gesprekken van medewerkers; dit verzoek, voorwaarde 9
De tijd die terugkomt, gaat naar de zorg	Dit verzoek, voorwaarde 10
Toetsset alleen met uw instemming	Verwerkersovereenkomst, art. 3.8; dit verzoek, voorwaarde 11

De pagina’s staan op axiomatic.digital/vertrouwen; de verwerkersovereenkomst met Axiomatic sturen wij mee.

Wat wij van u vragen

Wij leggen u het verzoek op de volgende pagina schriftelijk voor, met de redenen en de gevolgen voor medewerkers. Wij bespreken het met u in de overlegvergadering van [datum van de vergadering], vóór de uitrol naar meer teams na de pilot; zonder uw instemming volgen

geen andere teams en wordt Inora Matrix niet het officiële bekwaamheidsregister. Daarna besluit u, en laat u ons uw besluit schriftelijk en met redenen weten (artikel 27, lid 2 WOR). Hebt u vragen vooraf, dan beantwoorden wij die, of Axiomatic, in uw vergadering of op papier.

Met vriendelijke groet,

[Naam]
[Functie]

2. Het model voor het instemmingsverzoek

[Naam van de organisatie], de bestuurder
Aan de ondernemingsraad van [naam van de organisatie]
[Plaats], [datum]

Onderwerp: verzoek om instemming met de invoering van Inora (artikel 27, lid 1, onder k en l WOR)

Geachte leden van de ondernemingsraad,

Op grond van artikel 27 van de Wet op de ondernemingsraden vragen wij uw instemming met het voorgenomen besluit hieronder.

Artikel 1. Het voorgenomen besluit. Wij voeren Inora in, te beginnen met een pilot van acht weken in [naam van het team], van [startdatum] tot en met [einddatum]. Deelname aan de pilot is vrijwillig; Inora Matrix is tijdens de pilot een voorbeeldweergave voor het pilotteam. Voordat u hebt ingestemd, gaat geen ander team met Inora werken en wordt Inora Matrix niet het officiële bekwaamheidsregister. Na de pilot besluiten wij welke teams volgen. Dit besluit omvat de regeling voor het verwerken en beschermen van persoonsgegevens van medewerkers in Inora, met de voorwaarden in artikel 4.

Artikel 2. De beweegredenen. Zorgmedewerkers zoeken op hoe het bij ons moet, leggen vast wat zij deden en schrijven het uit, vaak na hun dienst. Inora neemt die drie stappen over, met antwoorden uit onze eigen protocollen en de bron erbij. Inora maakt de rapportage klaar; de medewerker leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft. Wij willen daarmee de administratietijd terugbrengen, de geldende werkafspraak op elk moment bereikbaar maken, ook ’s nachts, en de tijd teruggeven aan de cliënt.

Artikel 3. De gevolgen voor medewerkers. Medewerkers in de teams die met Inora werken, loggen in met hun eigen account. Zij stellen vragen in gewone taal en controleren het antwoord aan de bron; zij beslissen zelf. Niemand is verplicht een vraag aan Inora te stellen in plaats van aan een collega. Medewerkers krijgen een training bij de start. De pilot meet het effect per team, nooit per persoon.

Artikel 4. De voorwaarden. Wij voeren Inora alleen in onder deze voorwaarden:

1. Niemand in de organisatie leest het gesprek van een medewerker met Inora, ook de leiding niet.
2. Niemand in de organisatie krijgt een cijfer over één medewerker: niet hoe vaak, hoe snel of wanneer de medewerker werkt.
3. Inora beoordeelt niemand en geeft niemand een score.
4. Inora leidt geen emoties of stemming af.
5. Axiomatic leest een gesprek alleen in op schriftelijk verzoek van [functie, bijvoorbeeld de functionaris gegevensbescherming], voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.
6. Verslagen gaan over teams van minstens vijf mensen: per team naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams. Een kleiner team krijgt geen eigen verslag. Het onderwerp wordt tegelijk met het antwoord bepaald, zonder namen; geen mens leest mee.
7. Een vraag zonder antwoord gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg, naar de eigenaar van het onderwerp. Een onderwerp dat één keer gevraagd werd, gaat pas mee als het een tweede keer komt; na drie maanden gaat het alleen mee in de som over alle teams.
8. Een onjuist antwoord is een bevinding over Inora en de bron, nooit over de medewerker die het tegenkwam.

9. Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Dat dossier is onze bekwaamheidsregistratie voor voorbehouden en risicovolle handelingen volgens ons scholingsbeleid: de beoordelaar tekent de praktijktoets af, en daarna blijft het actueel met de handelingen die de medewerker zelf rapporteert, met het bijbehorende protocol en de geldende versie. Vragen van de medewerker aan Inora tellen nooit mee, ook niet als bewijs van bekwaamheid. Het legt de handeling, het protocol met zijn versie, de datum, in wiens opdracht en wie de praktijktoets aftekende vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. In de pilot is het dossier een voorbeeldweergave voor het deelnemende team en doen medewerkers vrijwillig mee; ons officiële register wordt het pas na uw instemming. Het staat in Inora zolang de medewerker bij ons werkt, plus 30 dagen; in die 30 dagen exporteren wij het naar ons eigen personeelsdossier. Het bekwaamheidsdossier zien bij ons alleen de teamleider en de opleiding, en de medewerker zelf. De medewerker ziet het eigen bekwaamheidsdossier in Inora en krijgt op verzoek een kopie. Het dossierlogboek toont, zodra Inora het dossier leest, via een koppeling of de eigen login, per stap wat Inora deed en namens wie. De functie die de organisatie aanwijst, ziet het alleen op schriftelijk verzoek, per cliënt of bij een onderzoek, ter controle op dossiertoegang; het is geen cijfer over een medewerker en bevat nooit wat iemand vraagt.
10. De tijd die Inora teruggeeft, gaat naar de zorg. Een besluit over de formatie is een eigen besluit, dat wij u apart voorleggen.
11. De toetsset zetten wij alleen aan als u daarmee hieronder apart instemt. Uit de toetsset leest geen mens een vraag of antwoord; de toets van een nieuwe versie is geautomatiseerd. Trekt u de instemming voor de toetsset in, dan verwijdert Axiomatic de toetsset binnen 30 dagen.

Voorwaarde 1 tot en met 9 en 11 staan ook in de verwerkersovereenkomst met Axiomatic, de privacyverklaring van Axiomatic (Gesprekken van medewerkers) en de pagina Inora en de AI-verordening (Wat Inora nooit doet). Voorwaarde 10 is een afspraak binnen onze organisatie en staat alleen in dit besluit. Axiomatic verzwakt geen voorwaarde zonder onze schriftelijke instemming.

Artikel 5. Evalueren. Wij evalueren de invoering met u na de pilot van acht weken en daarna elk jaar. U ontvangt daarvoor het maandverslag per team en een overzicht van elke inzage door Axiomatic (artikel 4, voorwaarde 5), zonder de inhoud ervan.

Artikel 6. Wijzigen. Willen wij iets aan deze voorwaarden veranderen, of Inora inzetten voor een ander doel, dan leggen wij u dat voor als een nieuw verzoek om instemming. Gebruiken wij Inora anders dan onder deze voorwaarden, dan is dat een besluit zonder uw instemming. U

kunt dan schriftelijk een beroep doen op de nietigheid, binnen een maand nadat wij u dat gebruik hebben meegedeeld of nadat het u is gebleken (artikel 27, lid 5 WOR), en wij stoppen dat gebruik.

Artikel 7. Ons verzoek. Wij vragen u in te stemmen met dit besluit, onder de voorwaarden in artikel 4. Wij bespreken het graag met u in de overlegvergadering van [datum van de vergadering], vóór de uitrol naar meer teams na de pilot. Na uw besluit laten wij u schriftelijk weten welk besluit wij nemen en per welke datum het ingaat.

Met vriendelijke groet,

[Naam], bestuurder van [naam van de organisatie]

Handtekening: _____

Besluit van de ondernemingsraad

In te vullen door de ondernemingsraad.

Veld	Invulling
Besproken in de overlegvergadering van	
Besluit over het verzoek	Instemming / geen instemming
Toetsset (voorwaarde 11)	Instemming / geen instemming
Redenen	
Datum en handtekening van de voorzitter	

AXIOMATIC

Kwaliteitsdossier

Inora, voor kwaliteit, de VAR en de directeur zorg

Dit dossier volgt het document over Inora en de AI-verordening en het leveranciersdossier. Bij verschil gaan de artikelen van de ondertekende overeenkomst voor.

Versie 1.8, 9 november 2026

1. Wat dit dossier regelt

Dit dossier is voor de kwaliteitsadviseur of -manager, de verpleegkundige adviesraad (VAR), de directeur zorg of specialist ouderengeneeskunde en de opleidingscoördinator van een zorgorganisatie die Inora beoordeelt. Het beantwoordt één vraag: komt elk antwoord uit ons eigen protocol? Ja, elk antwoord komt uit uw eigen protocol.

Het antwoord in één alinea. Inora antwoordt uit de afspraken van uw eigen organisatie en toont bij elke zin de bron, de versie en de passage. Staat het antwoord niet in uw bronnen, dan zegt Inora dat, en waar het zocht. De professional beslist; dat beoogde gebruik ligt woord voor woord vast en houdt Inora buiten de regels voor medische hulpmiddelen. Een document telt pas in Inora als het uw eigen route heeft doorlopen. Van elk antwoord legt Axiomatic vast waarop het rustte, zonder wie het vroeg. Gaat er iets mis, dan onderzoeken wij het systeem, nooit de professional.

2. Het beoogde gebruik

Wat een systeem mag doen, volgt uit het beoogde gebruik. Voor Inora luidt het, woord voor woord:

> Inora ondersteunt professionals met de kennis van hun organisatie. Het beantwoordt vragen uit uw bronnen en toont elke bron van uw organisatie met één tik, zet wat een professional zelf schreef in uw rapportageformats en toont wat uw protocollen nog vragen. Het maakt de opvolging klaar die daaruit volgt, zoals het verzoek aan de arts, de lijst in het dossier of de controle; die gaat alleen weg met het akkoord van de professional, en de professional beslist.

Inora stelt geen diagnose en beslist niet over een behandeling (art. 4.2). Daarbij: de professional beslist en is verantwoordelijk voor het besluit; een antwoord van Inora vervangt het oordeel van de professional niet (art. 4.3).

2.1 Triage

Inora ondersteunt triage. De verpleegkundige triageert, scoort en beslist. Inora legt het eigen protocol van de organisatie naast de verpleegkundige en wijst aan wat ontbreekt.

Stap	De verpleegkundige	Inora
Uitvragen	Ziet de cliënt, vraagt uit en meet.	Legt het triageprotocol van uw organisatie naast de verpleegkundige, vraag voor vraag.
Wat ontbreekt	Vult aan wat de verpleegkundige nog niet weet.	Wijst aan wat het protocol nog vraagt, zoals een ademfrequentie die niet is genoteerd.
Urgentie	Bepaalt hoe dringend het is.	Nooit.
Besluit	Besluit: zelf handelen, de arts bellen of de achterwacht.	Nooit.
Vastleggen	Leest en tekent de rapportage.	Maakt haar klaar, met het protocol en de versie die gold; na akkoord gaat zij het dossier in.

Inora maakt de rapportage klaar; de verpleegkundige leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft.

2.2 Wat Inora nooit doet

- Het stelt geen diagnose, geeft geen prognose en beslist niet over een behandeling.
- Het beoordeelt geen foto’s van huid of wonden.
- Het triageert niet in plaats van de verpleegkundige.
- Het beoordeelt geen medewerkers en neemt geen besluiten over hun werk.
- Het beslist niet of iemand recht heeft op een voorziening.
- Het leidt geen emoties of stemming van medewerkers af, niet uit stem en niet uit gezicht.

3. Waar Inora staat onder de wet

Regel	Wat het zegt	Wat het voor Inora betekent
Verordening (EU) 2017/745 (MDR), art. 2, punt 1	Software is een medisch hulpmiddel als de fabrikant haar bestemt voor een specifiek medisch doel, zoals diagnose, voorspelling of behandeling.	Inora is daar niet voor bestemd. Door zijn beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.
Verordening (EU) 2024/1689 (AI-verordening), art. 5, lid 1, onder f	Geen emotieherkenning op de werkplek, sinds 2 februari 2025.	Inora leidt geen emoties of stemming af.
AI-verordening, art. 4	AI-geletterdheid, sinds 2 februari 2025, gewijzigd per 27 juli 2026 (Verordening (EU) 2026/1744): aanbieders en gebruiksverantwoordelijken nemen maatregelen om de AI-geletterdheid te ondersteunen van hun personeel en van wie namens hen met het systeem werkt. Een bepaald niveau per persoon hoeven zij niet te garanderen.	Wij ondersteunen de AI-geletterdheid van wie met Inora werkt: wat het doet, wat het nooit doet en hoe een medewerker een bron controleert. Wij geven de training bij de invoering; uw organisatie krijgt het materiaal voor haar eigen maatregelen.
AI-verordening, art. 50, lid 4	Gepubliceerde AI-tekst wordt vermeld, sinds 2 augustus 2026.	Publiceert een organisatie toch AI-tekst om het publiek te informeren over een onderwerp van algemeen belang, dan vermeldt zij dat het AI-tekst is, tenzij een mens haar heeft getoetst en de organisatie of een medewerker de redactionele verantwoordelijkheid draagt.
AI-verordening, art. 25, lid 1, onder c	Wie een systeem buiten het beoogde gebruik inzet, kan zelf aanbieder van een systeem met een hoog risico worden.	Gebruik Inora binnen het beoogde gebruik van hoofdstuk 2.

Inora is geen hoog-risico AI-systeem: zorgprofessionals beoordelen en beslissen, Inora ondersteunt hen met de eigen protocollen van de organisatie. De medewerker ziet bij elk antwoord dat het door Inora is opgesteld, met de bron erbij; daarmee wordt invulling gegeven aan de transparantieplicht van artikel 50. U houdt bij wie is getraind om met Inora te werken, voor de plicht tot AI-geletterdheid van artikel 4.

Rollen onder de AI-verordening: Axiomatic B.V. is aanbieder; uw organisatie is gebruiksverantwoordelijke; de aanbieders van de modellen voor algemene doeleinden dragen de plichten voor hun modellen (art. 53).

Bronnen: MDR, AI-verordening, Verordening (EU) 2026/1744.

4. Wie waarvoor instaat

- **De zorgaanbieder** staat in voor goede zorg en voor de middelen die hij daarvoor inzet (Wet kwaliteit, klachten en geschillen zorg, art. 2 en 3). Dat blijft zo met Inora.
- **De professional** beslist en is verantwoordelijk voor het besluit.
- **Axiomatic** staat in voor wat Inora doet met uw bronnen; voor wat er in uw bronnen staat, staat uw organisatie in.

5. Hoe een antwoord tot stand komt, en wanneer Inora weigert

Elke zin van een antwoord rust op een bron van uw organisatie en eindigt in een markering. Eén tik op de markering toont de titel, de versie en de passage waaruit het antwoord komt. Staat het antwoord niet in de bronnen, dan zegt Inora dat, toont het waar het zocht en geeft het geen antwoord uit algemene kennis. De vraag gaat als onderwerp, zonder naam en zonder de woorden van wie vroeg, naar wie over het onderwerp gaat.

Een voorbeeld, zoals het op de pagina voor kwaliteit staat:

	Beantwoord	Niet in de bronnen
Vraag, 03:12 en 03:40	‘Ik sta vannacht alleen op de afdeling en moet morfine geven. Wie doet de dubbele controle?’	‘Mevrouw wil haar eigen CBD-olie innemen naast de morfine. Mag dat?’
Inora	De verpleegkundige van de bereikbaarheidsdienst, via beeldbellen in het toedienregistratiesysteem. Wordt er binnen 15 minuten niet opgenomen, bel dan de achterwacht en noteer dat de controle telefonisch was.	Dat staat niet in uw bronnen, dus daar geef ik geen antwoord op. Wel staat er: een zelfzorgmiddel naast voorgeschreven medicatie alleen na overleg met de apotheker.

	Beantwoord	Niet in de bronnen
Waar het op rust	Medicatiebeleid MED-04, 4.3, versie 7 (vastgesteld 12 juni 2026, eigenaar medicatiecommissie); Werkafspraak bereikbaarheid nacht ORG-12, 2, versie 3.	Gezocht in het Medicatiebeleid (5, Zelfzorgmiddelen), het Formularium 2026 en de Werkafspraak apotheek: geen passage. Als onderwerp, zonder naam, zonder de woorden van de zorgmede-werker en zonder cliënt naar de medicatiecommissie.

84% van de vragen over de risicothema's van de inspectie (medicatie, vrijheidsbeperking, wonden, vallen en infecties) vraagt om een eigen protocol. Daarom rust een antwoord op uw protocol, niet op algemene kennis.

6. Hoe een document in Inora komt

Een document komt in Inora zoals het in uw handboek komt.

Rol	Wat betrokkenen doen
De eigenaar	Elk document heeft er één bij u: een commissie, een team of een functie. Een vraag zonder antwoord komt als onderwerp bij de eigenaar terecht, zonder de naam en de woorden van wie vroeg.
Auteur en inhoudsdeskundigen	Schrijven en lezen mee zoals in uw eigen documentbeheer. Inora verandert geen letter.
Wie vaststelt	De kwaliteitsadviseur publiceert, of de VAR, zoals uw route het voorschrijft. Pas dan telt een document in Inora.
Concepten en oude versies	Tellen niet. Een vervangen versie blijft bewaard, zodat u kunt nagaan wat er op een dag gold.

Het verloop van één document:

Datum	Wie	Wat
9 maart 2026	Een vraag zonder antwoord	Onderwerp: dubbele controle 's nachts, alleen op de afdeling · 2×. Versie 6 zei het niet. Doorgestuurd naar de medicatiecommissie, zonder naam en zonder de woorden van de zorgmedewerker.

Datum	Wie	Wat
12 mei 2026	Specialist ouderengeneeskunde, auteur	Schrijft paragraaf 4.3 voor versie 7.
26 mei 2026	Apotheker en twee verpleegkundigen	Lezen mee als inhoudsdeskundigen.
12 juni 2026	Kwaliteitsadviseur, na advies van de VAR	Stelt vast en publiceert. Vanaf die dag antwoordt Inora uit versie 7; versie 6 telt niet meer.
2 november 2026	Een antwoord op dezelfde vraag	Rust op 4.3, versie 7.

7. Voor dag één: de intake van uw handboek

Elke invoering begint bij het kwaliteitshandboek, samen met uw kwaliteitsadviseur: wie eigenaar is van elk document, welke versie geldt en wat verlopen is. De uitkomst krijgt u per document, met de reden. In één kwaliteitshandboek van 350 documenten stonden 17 onderwerpen meer dan eens, en bij 8 daarvan zeggen de versies iets anders. Daarnaast waren 21 documenten over hun eigen herzieningsdatum, en stonden er bestanden in als plaatje dat geen zoekfunctie kan lezen (export van 24 september 2026, geteld op bestandshash, tekst en de kopvelden van het handboek).

Wat er met een bevinding gebeurt:

Wat de intake vindt	Wat ermee gebeurt
Twee versies van één onderwerp	De eigenaar kiest welke telt; de andere gaat eruit.
Herzieningsdatum verlopen	Naar de eigenaar, met de vraag of het nog geldt.
Opgeslagen als afbeelding	Omgezet in tekst; de eigenaar keurt die voordat hij telt.
Een wachtwoord of persoonsgegeven in een document	Naar de eigenaar, nooit in een antwoord.

Van elke bron die niet van uw organisatie is, staat in de licentielijst op welke grond Inora haar gebruikt.

8. Wat vastligt, en voor wie

Van elk antwoord legt Axiomatic vast waarop het rustte: de bronnen met hun versies, de toets die het doorstond en de datum, en een kenmerk dat de medewerker bij het antwoord ziet. Wie vroeg, het tijdstip en de afdeling staan er niet in, en het verslag blijft bij Axiomatic. Op schriftelijk verzoek, voor een incident of een klacht, krijgt u het.

U vraagt het op met de datum en de bron, of met dat kenmerk, dat de verpleegkundige zelf in de rapportage of MIC-melding kan zetten. Vraagt u binnen de bewaartermijn van het gesprek (standaard 90 dagen), dan zoeken wij langs dezelfde weg ook het gesprek na en houden het vast tot het onderzoek klaar is; daarna is er alleen het verslag, dat 2 jaar blijft. De medewerker hoort ervan dat het gesprek is ingezien.

Veld	Wat erin staat
Datum	De datum van het antwoord, niet het tijdstip.
Bronnen	Elk document met paragraaf, versie en datum van vaststelling.
Model	Het taalmodel dat het systeem koos, in de EU, met zijn versie.
Toetsset	De versie van uw toetsset die deze versie van Inora doorstond.
Kenmerk	Het kenmerk dat de verpleegkundige bij het antwoord ziet; het noemt niet wie vroeg.
Niet erin	Wie vroeg, het tijdstip, de afdeling, de vraag en het antwoord.

Het verslag staat bij Axiomatic in Europa (Ierland) en gaat na die termijn automatisch weg, binnen 30 dagen ook uit de back-ups.

Bij uw organisatie: wat een medewerker zelf verstuurt, zoals een rapportage of een MIC-melding; onderwerpen zonder antwoord, per eigenaar; gebruik per team van minstens vijf mensen, nooit per persoon; het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG), als eigen dossier met naam, los van elk antwoord.

Nooit bij uw organisatie: wie wat vroeg; het gesprek van een medewerker; een cijfer of score per persoon; hoe vaak één medewerker iets opzoekt; een bekwaamheid afgeleid uit een vraag of een antwoord. Het antwoordverslag blijft bij Axiomatic; u krijgt het op schriftelijk verzoek. Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die u daarvoor aanwijst, voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over

Inora, nooit wat de medewerker vroeg of las. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.

8.1 Het bekwaamheidsdossier

Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Dat dossier staat in Inora Matrix, uw bekwaamheidsregistratie voor voorbehouden en risicovolle handelingen volgens uw scholingsbeleid: de beoordelaar tekent de praktijktoets af, en daarna blijft het actueel met de handelingen die de medewerker zelf rapporteert, met het protocol en de versie die gold. Vragen van de zorgmedewerker aan Inora tellen nooit mee, ook niet als bewijs van bekwaamheid. In de pilot is het een voorbeeldweergave voor het deelnemende team, tot de ondernemingsraad instemt. Het is uw eigen dossier; Axiomatic bewaart het in Inora als verwerker, op uw instructie. Het is een eigen dossier met de naam van de medewerker, los van elk antwoord: Inora maakt het nooit op uit een vraag of uit het verslag van een antwoord. Het legt alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer. De bekwaamheid zelf stelt u vast, zoals uw scholingsbeleid voorschrijft.

Veld	Voorbeeld
Medewerker	Sanne de Wit, verzorgende IG
Handeling	Insuline subcutaan toedienen, voorbehouden handeling
Protocol	Insuline toedienen, versie 6
Datum	14 oktober 2026
In wiens opdracht	De behandelend arts van de cliënt

Het staat in Inora zolang de medewerker bij u werkt, plus 30 dagen; in die 30 dagen exporteert u het naar uw eigen personeelsdossier, waar uw eigen termijn geldt. Het bekwaamheidsdossier zien alleen uw teamleider en uw opleiding, en de medewerker zelf. De medewerker ziet het eigen bekwaamheidsdossier altijd in Inora en krijgt op verzoek een kopie: dat is het recht op inzage (artikel 15 AVG), dat u beantwoordt en waarbij Axiomatic helpt. Artikel 5.6 van de verwerkersovereenkomst„ bindt het.

9. Het systeem staat centraal in elk onderzoek

Een fout in een antwoord komt uit het systeem: uit een bron die verouderd is, uit een versie van het model, uit de software eromheen, uit een instelling of uit onze eigen werkwijze. Daar zoeken wij de oorzaak, nooit bij de professional die de fout tegenkwam. Vijf stappen, elke keer:

1. **Melden.** Wij melden de fout eerst aan wie hij raakt; een datalek uiterlijk 24 uur na kennisname.
2. **Herstellen.** Het werk gaat terug naar een versie die werkt, waar nodig de vorige.
3. **Onderzoeken.** Zonder schuldvraag: in de bron, het model, de software eromheen, de inrichting en onze eigen werkwijze. Geen bevinding noemt wie de fout tegenkwam.
4. **Opschrijven.** Wat wij vinden, krijgt uw organisatie op papier. Loopt het onderzoek nog, dan vullen wij het aan.
5. **Veranderen.** De verandering gaat in het systeem, met een toets die voorkomt dat dezelfde fout er ongemerkt opnieuw doorkomt.

Na een calamiteit levert Axiomatic binnen 5 werkdagen een eerste bevinding en binnen 4 weken een verslag, binnen de acht weken die de inspectie u voor uw eigen onderzoek geeft (Uitvoeringsbesluit Wkkgz, art. 8.7, lid 2), na uw melding (Wkkgz, art. 11).

9.1 Uw toetsset, voor elke nieuwe versie

Elke nieuwe versie toetsen wij op de eigen vragen van uw organisatie voordat uw medewerkers ermee werken: echte vragen, ontdaan van namen van cliënten en medewerkers, alleen op uw schriftelijke opdracht, na instemming van de ondernemingsraad waar u er een heeft; geen mens leest ze. Elke eerdere fout komt erin als toets die blijft. Doet een versie het op één vraag slechter dan de vorige, dan wordt hij tegengehouden, hersteld en opnieuw getoetst.

9.2 Beschikbaar, dag en nacht

Ook ’s nachts. Uw bronnen blijven in uw eigen documentsysteem staan; Inora werkt met een kopie die uw handboekbeheerder aanlevert en bijwerkt. Inora is ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht.

10. Wat uw organisatie doet

- Gebruik Inora binnen het beoogde gebruik van hoofdstuk 2.
- Wijs uw bronnen aan en houd ze actueel. Elk document heeft een eigenaar bij u.
- Neem maatregelen om de AI-geletterdheid van uw medewerkers te ondersteunen (AI-verordening, art. 4, gewijzigd per 27 juli 2026). Wij geven de training bij de invoering.
- Laat de professional beslissen.
- Betrek uw ondernemingsraad (Wet op de ondernemingsraden, art. 27, lid 1, onder k en l).
- Vermeld AI-tekst die u publiceert.
- Meld wat misgaat.

11. Wat u van ons krijgt

Stuk	Wanneer
Het beoogde gebruik, woord voor woord	Vóór de eerste vraag
Dit kwaliteitsdossier	Vóór de eerste vraag
De uitkomst van de intake van uw handboek, per document met de reden	Vóór dag één
De licentielijst	Vóór dag één
Het trainingsmateriaal voor AI-geletterdheid	Bij de invoering
Het verslag van een fout, met de bevinding en de toets	Bij elk incident

Contact: support@axiomatic.digital. Axiomatic B.V., Delft, KvK-nummer 97816825.

12. Inora en de AI-verordening, volledig

Dit document beschrijft Inora voor de AI-verordening, Verordening (EU) 2024/1689: voor de organisaties die Inora inzetten, hun functionaris gegevensbescherming, hun ondernemingsraad en wie op hen toeziet.

Over dit document

- **Systeem:** Inora
- **Aanbieder:** Axiomatic B.V., Delft, KvK-nummer 97816825
- **Contact:** support@axiomatic.digital

Wij werken dit document bij als Inora, de modellen die het gebruikt of de regels veranderen, en na een ernstig incident.

Wie welke rol heeft

- **Aanbieder.** Axiomatic ontwikkelt Inora en brengt het onder eigen naam in de handel. Onder de AI-verordening dragen wij de plichten van de aanbieder.
- **Gebruiksverantwoordelijke.** Elke organisatie die Inora onder haar eigen gezag gebruikt, is gebruiksverantwoordelijke. Haar medewerkers werken ermee.
- **Aanbieders van modellen.** Inora gebruikt AI-modellen voor algemene doeleinden van andere aanbieders. Die aanbieders dragen de plichten voor hun modellen, zoals artikel 53 ze vastlegt.

Inora is geen hoog-risico AI-systeem: de zorgprofessional beoordeelt en beslist, Inora ondersteunt met de eigen protocollen van de organisatie. Het beoogde gebruik van Inora valt in geen categorie van bijlage III. Bijlage III, punt 5, onder d, noemt systemen voor de triage van patiënten in de spoedeisende zorg; Inora triageert niet en bepaalt geen prioriteit. De verpleegkundige doet dat, en Inora legt het protocol van de organisatie ernaast.

De medewerker ziet bij elk antwoord dat het door Inora is opgesteld, met de bron erbij; daarmee wordt invulling gegeven aan de transparantieplicht van artikel 50. U houdt bij wie is getraind om met Inora te werken, voor de plicht tot AI-geletterdheid van artikel 4.

Het beoogde gebruik

Wat een systeem mag doen, volgt uit het beoogde gebruik. Voor Inora luidt het, woord voor woord:

> Inora ondersteunt professionals met de kennis van hun organisatie. Het beantwoordt vragen uit uw bronnen en toont elke bron van uw organisatie met één tik, zet wat een professional zelf schreef in uw rapportageformats en toont wat uw protocollen nog vragen. Het bereidt de opvolging voor die daaruit volgt, zoals het verzoek aan de arts, de lijst in het dossier of de controle; die gaat alleen weg met het akkoord van de professional, en de professional beslist.

Inora stelt geen diagnose en beslist niet over een behandeling. Door zijn beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.

Wat Inora nooit doet

- Het stelt geen diagnose, geeft geen prognose en beslist niet over een behandeling.
- Het beoordeelt geen foto's van huid of wonden.
- Het doet geen triage van patiënten. De verpleegkundige triageert; Inora ondersteunt met het eigen protocol van de organisatie en wijst aan wat ontbreekt.
- Het beoordeelt geen medewerkers en neemt geen besluiten over hun werk. Cijfers over gebruik gaan alleen over teams van minstens vijf mensen, nooit over één medewerker, en niemand krijgt een score. Het bekwaamheidsdossier gaat alleen over voorbehouden en risicovolle handelingen volgens het scholingsbeleid van de organisatie; het is van de organisatie, legt de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer, en vragen van medewerkers aan Inora tellen nooit mee. De medewerker ziet het eigen bekwaamheidsdossier in Inora en krijgt op verzoek een kopie (artikel 15 AVG); wat dat voor de ondernemingsraad betekent, staat op Ondernemingsraad.
- Het beslist niet of iemand recht heeft op een voorziening.
- Het leidt geen emoties of stemming van medewerkers af, niet uit stem en niet uit gezicht. Dat verbiedt artikel 5, lid 1, onder f.

Wie een AI-systeem inzet voor een gebruik buiten het beoogde gebruik, kan daardoor zelf aanbieder van een AI-systeem met een hoog risico worden (artikel 25, lid 1, onder c).

Plichten die nu gelden

- **AI-geletterdheid** (artikel 4, sinds 2 februari 2025, gewijzigd per 27 juli 2026 door Verordening (EU) 2026/1744). Aanbieder en gebruiksverantwoordelijke nemen maatregelen om de AI-geletterdheid te ondersteunen van wie namens hen met het systeem werkt; een bepaald niveau per persoon hoeven zij niet te garanderen. Wie met Inora werkt, leert wat het doet, wat het nooit doet en hoe hij een bron controleert. Wij geven de training bij de invoering, en de organisatie krijgt het materiaal voor haar eigen maatregelen. Sinds dezelfde datum geldt het verbod op emotieherkenning op het werk (artikel 5, lid 1, onder f); hoe Inora dat volgt, staat onder Wat Inora nooit doet.
- **AI-tekst die een organisatie publiceert** (artikel 50, lid 4, sinds 2 augustus 2026). Publiceert een organisatie toch AI-tekst om het publiek te informeren over een onderwerp van algemeen belang, dan vermeldt zij dat het AI-tekst is, tenzij een mens haar heeft getoetst en de organisatie of een medewerker de redactionele verantwoordelijkheid draagt.

De professional houdt het overzicht

De professional beslist. Inora is zo gebouwd dat de professional ziet waar een antwoord op rust, en het kan tegenspreken:

- Elke bron van de organisatie is in het antwoord gemarkeerd. Eén tik op de markering toont de titel, de versie en de passage waaruit het antwoord komt.
- Staat het antwoord niet in de bronnen, dan zegt Inora dat, en waar het zocht. Het onderwerp gaat, zonder naam en zonder de woorden van de professional, naar de eigenaar van de bron, zodat de bron kan worden aangevuld.
- In een rapportage komen de woorden van de professional onder de kopjes van de organisatie. Inora schrijft de rapportage als concept; de professional leest en tekent, en pas op dat akkoord zet Inora die in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft.
- Inora handelt pas als een mens akkoord geeft.

Waar het draait

Inora draait in de EU of op de eigen servers van uw organisatie. Het systeem kiest per taak het taalmodel; de leverancier staat op de pagina Subverwerkers. Elke nieuwe versie wordt getoetst voordat medewerkers ermee werken; op schriftelijke opdracht van de organisatie ook op haar eigen toetsset.

Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU, of op de eigen servers van een organisatie binnen haar netwerk. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek.

Niemand traint of verfijnt een model met de documenten, vragen, antwoorden of rapportages van een organisatie: wij niet, en geen enkele aanbieder van een model.

Gegevens	Van wie	Waarvoor
Bronnen: documenten, protocollen, werkafspraken	De organisatie	De antwoorden
Gesprekken: vragen, antwoorden en rapportages, en het onderwerp van elk gesprek, zonder namen	De medewerkers van de organisatie	Het gesprek zelf, en het onderwerp voor de teamverslagen, in dezelfde stap als het antwoord ingedeeld; standaard 90 dagen bewaard. Vraagt de organisatie binnen de bewaartermijn dat Axiomatic een gesprek inziet voor een incident of een klacht, dan houdt Axiomatic het vast tot het onderzoek is afgerond en verwijdert het daarna binnen 30 dagen; de medewerker hoort ervan
Antwoordverslag: per antwoord de bronnen met hun versies, de toets en de datum, en een kenmerk dat de medewerker bij het antwoord ziet; nooit wie vroeg, het tijdstip, de afdeling, de vraag of het antwoord	Axiomatic, van elk antwoord	Verantwoorden waarop een antwoord rustte, bij een incident of een klacht; 2 jaar, bij Axiomatic
Toetsset: vragen uit de organisatie en gemarkeerde antwoorden met hun vraag, ontdaan van namen van cliënten en medewerkers	De organisatie, alleen op haar schriftelijke opdracht, na instemming van de onderne-mingsraad waar zij er een heeft	Elke nieuwe versie toetsen voordat die live gaat; geen mens leest daarvoor een vraag of antwoord; bewaard tot zij de opdracht intrekt, uiterlijk tot het einde van de overeenkomst, daarna binnen 30 dagen verwijderd

Wat wij verwerken en waarom, staat in het privacyverklaring.

Voor organisaties die Inora inzetten

- **Gebruik Inora binnen het beoogde gebruik.** Zet het in ter ondersteuning van triage, nooit om in plaats van de professional te triageren; zet het niet in voor het beoordelen van medewerkers of het toekennen van voorzieningen, en laat het geen foto's van huid of wonden beoordelen.
- **Wijs uw bronnen aan en houd ze actueel.** Wat Inora over uw organisatie zegt, rust op de bronnen die u aanwijst. Elk document heeft een eigenaar bij u. Een verouderd protocol geeft een verouderd antwoord.
- **Ondersteun de AI-geletterdheid van uw medewerkers** (artikel 4, zoals gewijzigd door Verordening (EU) 2026/1744). Wie met Inora werkt, leert wat het doet, wat het nooit doet en hoe hij een bron controleert. Wij geven de training bij de invoering.
- **Laat de professional beslissen.** Inora ondersteunt; het besluit neemt de professional.
- **Betrek uw ondernemingsraad.** De ondernemingsraad heeft instemmingsrecht bij een systeem dat persoonsgegevens van medewerkers verwerkt of hun gedrag of prestaties kan waarnemen (artikel 27, lid 1, onder k en l, van de Wet op de ondernemingsraden).
- **Vermeld AI-tekst die u publiceert,** zoals hierboven onder artikel 50, lid 4.
- **Meld wat misgaat.** Antwoordt Inora verkeerd, gaat het over de grens van het beoogde gebruik, of weigert het een vraag die uw bronnen beantwoorden, meld het dan aan uw kwaliteitsteam en aan ons.

13. De licentielijst

Van elke bron die niet van uw organisatie is, staat erin op welke grond Inora haar gebruikt. Op een landelijke referentie laat Inora een antwoord alleen rusten waar de uitgever dat toestaat. De zorgmedewerker ziet haar niet, zonder markering en zonder link; bij het antwoord ligt zij wel vast. De naamsvermelding die een open licentie vraagt, staat op een vaste pagina in de juridische informatie van Inora.

AXIOMATIC

Privacyverklaring

Wij verkopen geen persoonsgegevens, gebruiken ze niet voor reclame en trainen geen model met gegevens van organisaties. Niemand in een organisatie leest de gesprekken van haar medewerkers met Inora. Hieronder staat wat wij verwerken op onze website, bij uw contact met ons en in Inora, waarom, waar en hoe lang, wie het nog meer verwerkt en welke rechten u hebt.

Bijgewerkt op 9 november 2026

Wie wij zijn

Axiomatic B.V. is een softwarebedrijf in Delft, ingeschreven in het Handelsregister van de Kamer van Koophandel onder nummer 97816825. Wij ontwerpen en bouwen Inora, voeren het zelf in en beheren het.

Onze functionaris gegevensbescherming is een externe FG, bereikbaar via fg@axiomatic.digital en aangemeld bij de Autoriteit Persoonsgegevens. Met andere vragen over deze verklaring kunt u terecht bij privacy@axiomatic.digital.

Twee rollen: voor onszelf en voor zorgorganisaties

In deze verklaring onderscheiden wij twee rollen uit de AVG. De verwerkingsverantwoordelijke bepaalt waarom en hoe gegevens worden verwerkt. De verwerker verwerkt gegevens in opdracht en volgens de instructies van de verwerkingsverantwoordelijke.

Voor ons eigen werk zijn wij verwerkingsverantwoordelijke. Dat geldt voor de website, voor e-mail die u ons stuurt, voor onze relatie met klanten en potentiële klanten en voor sollicitaties. De onderdelen ‘De website’ tot en met ‘In één overzicht’ gaan hierover.

Voor Inora is de zorgorganisatie verwerkingsverantwoordelijke en zijn wij verwerker. De organisatie bepaalt voor welke doeleinden zij Inora gebruikt, welke documenten erin staan, welke medewerkers ermee werken en hoe lang gesprekken bewaard blijven. Wij verwerken die gegevens alleen volgens de instructies van de organisatie, onder een verwerkersovereenkomst

die voldoet aan artikel 28 van de AVG. Het onderdeel ‘Inora: wat wij in opdracht van zorgorganisaties verwerken’ gaat hierover. Die uitleg komt niet in de plaats van de privacyverklaring van de zorgorganisatie of van de verwerkersovereenkomst.

Werkt u bij een zorgorganisatie die Inora gebruikt, of ontvangt u daar zorg, dan bepaalt die organisatie wat er met uw gegevens gebeurt. Stel uw vraag eerst aan de organisatie. Neemt u contact met ons op, dan sturen wij uw verzoek door naar de organisatie en helpen wij haar bij het antwoord.

De website

Wij willen weten hoe onze website wordt gelezen, en door welke organisaties. Daarvoor gebruiken wij PostHog, een dienst voor webanalyse. Het script van PostHog zit in de bestanden van onze eigen website en stuurt via ons eigen domein naar de EU-cloud van PostHog.

Wat PostHog ontvangt. Welke pagina’s u bekijkt, hoe ver u leest en wanneer u weggaat; waar u klikt, wat u kopieert en welke documenten u downloadt; een opname van uw bezoek, met wat u ziet, waar u beweegt en klikt en wat u in een formulier typt, ook voordat u op Versturen drukt; de verzoeken die de pagina doet, met hun inhoud, hun headers en hun laadtijd; meldingen en fouten in de console van de browser; de laadsnelheid van de pagina (Web Vitals); de pagina, zoekmachine of campagne waarvandaan u kwam; uw IP-adres, dat wij niet inkorten, en uw browser. Een kenmerk in een cookie en in de lokale opslag van uw browser koppelt uw bezoeken aan elkaar.

Wanneer wij weten wie u bent. Verstuurt u een formulier, dan koppelt PostHog uw bezoeken, ook de eerdere, aan het e-mailadres, de naam, de functie en de organisatie die u invulde. Opent u een link die wij u persoonlijk stuurden, dan staat daarin een code die alleen wij met uw naam kunnen verbinden; ook dan komen uw bezoeken bij uw gegevens. Bezoekers met een zakelijk e-mailadres van dezelfde organisatie brengen wij in PostHog samen onder die organisatie.

Van welke organisatie een bezoek komt. Bij bezoeken die wij niet aan een naam kunnen koppelen, vragen wij IPinfo achteraf bij welke organisatie het IP-adres hoort, en zetten wij die organisatie bij het bezoek. Dat gebeurt op onze servers, niet in uw browser.

De chat. Zodra u op een pagina scrolt, klikt of een toets indrukt, laadt de chat van Intercom, van de domeinen van Intercom. Vanaf dat moment ontvangt Intercom uw IP-adres, uw browser, de pagina die u bekijkt en wat u in de chat schrijft. Hebt u een formulier verstuurd, dan

krijgt de chat ook uw naam en e-mailadres, zodat wij u daar kunnen antwoorden. In de chat antwoordt eerst Ax, een AI-assistent (Fin, van Intercom), uit de openbare pagina's van deze website; elk antwoord van Ax draagt het label 'AI Agent'. Ons team leest mee en neemt het gesprek over als u daarom vraagt.

Waarom. Om te zien hoe de website wordt gebruikt en waar zij tekortschiet; om te weten welke organisaties zich in Inora verdiepen, zodat wij hen op het goede moment en met de goede informatie kunnen helpen; en om u in de chat te antwoorden. Grondslag: ons gerechtvaardigd belang (artikel 6, lid 1, onder f AVG). Wij gebruiken deze gegevens niet voor advertenties, verkopen ze nooit, en ze komen nooit in Inora.

Wie het verwerkt. PostHog, Inc. (Verenigde Staten), in zijn EU-cloud: de gegevens staan in Duitsland, bij Amazon Web Services. Intercom R&D Unlimited Company (Ierland): de chat staat in de Verenigde Staten, bij Intercom, Inc. en Amazon Web Services. IPinfo, Inc. (Verenigde Staten), dat alleen het IP-adres ontvangt. Alle drie verwerken de gegevens als onze verwerker en staan op Subverwerkers. PostHog en Intercom, Inc. nemen deel aan het EU-VS-kader voor gegevensbescherming (Data Privacy Framework), en hun verwerkersovereenkomsten voegen de standaardcontractbepalingen van de EU toe (posthog.com/dpa, posthog.com/subprocessors, intercom.com/legal/data-processing-agreement).

Hoe lang. Opnamen bewaren wij 30 dagen. Gebeurtenissen en het bezoekersprofiel, met de naam, het e-mailadres en de organisatie die eraan gekoppeld zijn, bewaart PostHog zeven jaar, de termijn van ons abonnement (posthog.com/docs/data/events-retention). Chatgesprekken bij Intercom bewaren wij tot twee jaar na het laatste contact, net als onze e-mail. Op uw verzoek verwijderen wij alles eerder.

Bezwaar maken. Schrijf naar privacy@axiomatic.digital met de datum en het tijdstip van uw bezoek, of met het e-mailadres dat u invulde. Dan verwijderen wij uw opnamen, gebeurtenissen en profiel bij PostHog, en uw gesprekken bij Intercom (artikel 21 AVG). U kunt het ook zelf tegenhouden: zet JavaScript uit voor axiomatic.digital, dan gaat er niets naar PostHog of Intercom, en elke pagina is ook dan te lezen. Blokkeert u alleen cookies en lokale opslag, dan koppelt PostHog uw bezoeken niet meer aan elkaar, maar neemt het elk bezoek nog wel op.

Lettertypen, afbeeldingen, opmaak en het script van PostHog komen van ons eigen domein. Alleen de chat laadt van de domeinen van Intercom, en pas nadat u scrolt, klikt of typt.

De website wordt gehost bij Amazon Web Services: de bestanden staan in de regio Europa (Ierland) en Amazon CloudFront levert ze af. Om een pagina te leveren en de website tegen aanvallen te beschermen, verwerkt CloudFront de technische gegevens die bij elk verzoek

horen: uw IP-adres, de opgevraagde pagina, het tijdstip en de identificatie van uw browser. Wij zetten geen toegangslogs aan en houden er zelf geen bij. CloudFront kan een pagina leveren vanaf een locatie buiten de Europese Unie; zie ‘Waar de gegevens staan’.

Grondslag voor dit leveren en beveiligen: ons gerechtvaardigd belang (artikel 6, lid 1, onder f AVG).

E-mail en contact

Mailt u ons, dan bewaren wij uw bericht, uw naam, uw e-mailadres en wat u verder meestuurt, zodat wij kunnen antwoorden en de voorgeschiedenis bij de hand hebben als u opnieuw schrijft. Onze e-mail loopt via Google Workspace.

Wij bewaren correspondentie tot twee jaar na het laatste contact, tenzij die onderdeel wordt van een klantrelatie of de wet een langere termijn voorschrijft.

Grondslag: ons gerechtvaardigd belang om u te antwoorden (artikel 6, lid 1, onder f AVG). Gaat het om stappen die u vraagt voor een overeenkomst waarbij u zelf partij bent, dan geldt artikel 6, lid 1, onder b AVG. Een overeenkomst met uw werkgever is geen overeenkomst met u.

U bepaalt zelf of u ons mailt en wat u meestuurt. Zonder voldoende contactgegevens en uitleg kunnen wij uw vraag mogelijk niet beantwoorden. Stuur geen cliëntgegevens mee.

Als u het contactformulier invult

Wat wij ontvangen. Via ‘Praat met ons team’ op elke pagina en op /contact ontvangen wij uw e-mailadres, voornaam, achternaam, functie, organisatie, omvangklasse in fte, zorgveld en uw antwoord op ‘Welk werk kost uw team nu de meeste tijd?’. Ook ontvangen wij de taal, het tijdstip, de pagina waarop u het formulier opende en wat die pagina meegaf: veld, route en aantal zorgmedewerkers. Wij vragen geen telefoonnummer.

Wat naar PostHog en Intercom gaat. De opname van uw bezoek bevat het formulier zoals u het invult, en het verzoek waarmee het wordt verstuurd, met de inhoud. Na het versturen koppelt PostHog uw bezoeken aan uw e-mailadres, naam, functie en organisatie, en brengt het u samen met anderen van uw organisatie (zie ‘De website’). De chat van Intercom krijgt uw naam en e-mailadres.

Waarom. Wij verwerken deze gegevens om u te antwoorden, op grond van ons gerechtvaardigd belang (artikel 6, lid 1, onder f AVG). Gaat het om stappen voor een overeenkomst, dan geldt artikel 6, lid 1, onder b AVG.

Hoe lang. Axiomatic bewaart de gegevens twaalf maanden; daarna verwijdert het systeem ze vanzelf. Een kopie kan nog 35 dagen in de back-up staan. De e-mail zelf bewaren wij als correspondentie; zie ‘E-mail en contact’.

Wie het ontvangt. Ons team ontvangt uw bericht per e-mail. Opslag en verzending lopen via Amazon Web Services in de regio Europa (Ierland); de e-mail komt binnen bij Google Workspace. Beide staan op Subverwerkers.

Verwijderen of inzien. Schrijf naar privacy@axiomatic.digital.

Als u de AI-scan invult

De AI-scan op /scan rekent uw uitkomst uit in uw eigen browser. Uw antwoorden komen pas als aanvraag bij ons binnen wanneer u op Versturen drukt. Wel neemt PostHog, zoals op elke pagina, uw bezoek op, ook wat u in de scan aanklikt en typt voordat u verstuurt (zie ‘De website’). Ook het e-mailveld zit in die opname, net als het verzoek dat de pagina bij het versturen doet, met uw antwoorden en uw e-mailadres. De scan zelf zet geen eigen cookie. De eerste vraag van de scan staat ook op Starten met Inora: kiest u daar een antwoord, dan gaat het in het adres van de pagina mee naar de scan, en dat adres ziet PostHog ook.

Wat wij ontvangen als u op Versturen drukt. Uw antwoorden op de tien vragen, de uitkomst die daaruit volgt, de taal van de pagina en het tijdstip, en wat u eventueel koos op de pagina waarvandaan u naar de scan kwam. Vult u uw e-mailadres in, dan ontvangen wij dat ook. In de opslag van de scan bewaren wij uw IP-adres niet. Om misbruik te beperken, tellen wij wel hoeveel verzoeken er binnen een uur van hetzelfde adres komen, onder een gezouten hash van dat adres, los van uw antwoorden. Het zout wisselt elk uur, en na dat uur gebruiken wij de hash niet meer; het systeem wist hem vanzelf, doorgaans binnen enkele dagen, en een kopie kan nog 35 dagen in onze back-up staan.

Wat ook naar PostHog gaat. Bij het versturen gaat een kopie van uw antwoorden en de uitkomst naar PostHog, met uw IP-adres, uw browser en het land waaruit u de pagina opvroeg, gekoppeld aan uw bezoek. Vult u uw e-mailadres in, dan koppelt PostHog uw bezoeken daaraan (zie ‘De website’). Voor die kopie geldt dezelfde toestemming; trekt u haar in, dan verwijderen wij ook uw profiel en gebeurtenissen bij PostHog.

Waarom. Wij gebruiken uw antwoorden en, als u het invult, uw e-mailadres om u de uitkomst te sturen en er contact over op te nemen, op basis van uw toestemming, die u geeft door op Versturen te drukken; u kunt die altijd intrekken.

Hoe lang. Bij Axiomatic bewaren wij de antwoorden en het e-mailadres twaalf maanden; daarna verwijdert het systeem ze vanzelf, en een kopie kan nog 35 dagen in onze back-up staan. De e-mail met uw antwoorden in onze mailbox bewaren wij als correspondentie (zie ‘E-mail en contact’). De kopie bij PostHog blijft, net als de rest van uw bezoek, zeven jaar, de termijn van ons abonnement bij PostHog, tenzij u vraagt haar eerder te verwijderen; dan verwijderen wij uw profiel en uw gebeurtenissen bij PostHog.

Wie het ontvangt. Bij Axiomatic alleen Ahsan Fazal, die de scan beantwoordt. De opslag en het versturen lopen via Amazon Web Services in de regio Europa (Ierland); de e-mail komt binnen in onze mailbox bij Google Workspace; PostHog ontvangt de kopie hierboven. Alle drie staan op Subverwerkers. Wij verkopen uw gegevens niet en delen ze met niemand anders.

Verwijderen of inzien. Schrijf naar privacy@axiomatic.digital vanaf het adres dat u invulde, of noem het. Dan verwijderen wij uw gegevens, ook bij PostHog. Op dezelfde manier vraagt u om inzage of correctie. Bent u het niet eens met hoe wij met uw gegevens omgaan, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

Klanten en potentiële klanten

Per organisatie waarmee wij werken, bewaren wij de namen, zakelijke e-mailadressen, telefoonnummers en functies van onze contactpersonen, de overeenkomsten die wij sluiten en onze facturen. Die hebben wij nodig om de overeenkomst voor te bereiden, uit te voeren en te factureren. Wij ontvangen contactgegevens van u of van uw organisatie.

Contactgegevens bewaren wij zolang de relatie duurt en tot twee jaar daarna. Facturen en de administratie daarachter bewaren wij zeven jaar, omdat de fiscale bewaarplicht dat voorschrijft.

Grondslag: ons gerechtvaardigd belang om samen te werken met de organisatie waar u werkt (artikel 6, lid 1, onder f AVG) en onze wettelijke plicht om een administratie te bewaren (artikel 6, lid 1, onder c AVG).

Axiomatic neemt geen betaalkaarten aan. Klanten betalen per bankoverschrijving op factuur.

Solliciteren

Solliciteert u bij Axiomatic, dan bewaren wij uw brief, cv, correspondentie en aantekeningen van gesprekken. Alleen wie bij de selectie betrokken is, ziet ze. Zonder de informatie die voor de functie nodig is, kunnen wij uw sollicitatie niet beoordelen.

Wij verwijderen uw gegevens uiterlijk vier weken na het einde van de procedure. Met uw toestemming bewaren wij ze tot een jaar na het einde van de procedure, zodat wij u kunnen benaderen voor een andere functie. U kunt die toestemming altijd intrekken.

Grondslag: stappen voorafgaand aan een arbeidsovereenkomst (artikel 6, lid 1, onder b AVG); voor de langere termijn uw toestemming (artikel 6, lid 1, onder a AVG).

In één overzicht

Gegevens	Doel	Grondslag	Bewaartermijn
Technische verzoekgegevens van de website (IP-adres, pagina, tijdstip, browser)	De website leveren en beveiligen	Gerechtvaardigd belang	Geen toegangslogs bij Axiomatic
Websitebezoek in PostHog (pagina's, klikken, een opname van het bezoek met wat u typt, herkomst, IP-adres, browser; na een formulier of een persoonlijke link uw naam, e-mailadres, functie en organisatie)	Zien hoe de website wordt gebruikt en door welke organisaties	Gerechtvaardigd belang	Opnamen 30 dagen; gebeurtenissen en bezoekersprofiel zeven jaar, op verzoek eerder weg
De organisatie bij een IP-adres (IPinfo)	Weten van welke organisatie een bezoek komt	Gerechtvaardigd belang	Bij het bezoekers-profiel in PostHog, zeven jaar
De chat (Intercom)	U antwoorden	Gerechtvaardigd belang	Twee jaar na het laatste contact
De verstuurde AI-scan (antwoorden, uitkomst, e-mailadres als u het invult)	U de uitkomst sturen en contact over de uitkomst	Toestemming	Twaalf maanden bij Axiomatic; de kopie bij PostHog zeven jaar; op verzoek eerder weg

Gegevens	Doel	Grondslag	Bewaartermijn
Het verstuurde contactformulier (contact- en organisatiegegevens, functie, omvangklasse, zorgveld, bericht)	Uw bericht beantwoorden en stappen voor een overeenkomst	Gerechtvaardigd belang; stappen voor een overeenkomst	Twaalf maanden bij Axiomatic; daarna nog maximaal 35 dagen in de back-up
E-mailcorrespondentie	Antwoorden en de voorgeschiedenis bewaren	Gerechtvaardigd belang; stappen voor een overeenkomst	Twee jaar na het laatste contact
Contactgegevens van medewerkers van klanten	Overeenkomsten voorbereiden en uitvoeren	Gerechtvaardigd belang	Duur van de relatie plus twee jaar
Facturen en administratie	Factureren en fiscale verplichtingen	Wettelijke plicht	Zeven jaar
Sollicitaties	Selectie	Stappen voor een overeenkomst; toestemming voor langer bewaren	Vier weken na de procedure; een jaar met toestemming
Gegevens in Inora	In opdracht van de zorgorganisatie	Bepaald door de organisatie als verwerkingsverantwoordelijke	Zie ‘Inora’ en ‘Bewaren en verwijderen’

Inora: wat wij in opdracht van zorgorganisaties verwerken

Met Inora stellen zorgmedewerkers een vraag in gewone taal en krijgen zij antwoord uit de bronnen van hun organisatie. Elke bron van de organisatie is in het antwoord gemarkeerd, en de passage staat één tik verder. Daarvoor verwerkt Inora per organisatie twaalf soorten gegevens, in de volgorde van bijlage 1 van de verwerkersovereenkomst.

1. Documenten. De protocollen, richtlijnen, werkafspraken, procedures en het kwaliteitshandboek die de organisatie toevoegt. Daarin kunnen namen van medewerkers staan, bijvoorbeeld van auteurs en eigenaren.

2. Vragen, antwoorden en rapportages. Vragen kunnen getypt of ingesproken zijn. Wat gebruikers vragen, wat Inora antwoordt, welke bronnen het toont en de rapportages die het opstelt in het format van de organisatie, zoals SBAR, SOAP of SOEP.

Voor de teamverslagen (zie ‘Gesprekken van medewerkers’) deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, zonder namen. Geen mens leest mee, en de indeling blijft in de omgeving en verdwijnt met het gesprek.

3. Gebruikersaccounts. Inora ontvangt de naam, het zakelijke e-mailadres, een unieke code en de groepen van een gebruiker uit de eigen single sign-on van de organisatie. Met single sign-on bewaart Inora geen wachtwoorden.

4. Logging. Inlogmomenten, beheerhandelingen en technische gegevens zoals IP-adressen en tijdstippen, om de dienst veilig te houden en problemen te onderzoeken.

Op verzoek krijgt de organisatie de logging alleen opgeteld per team van minstens vijf mensen en per dag; inlogmomenten en IP-adressen van één medewerker nooit. Bij een beveiligingsincident onderzoeken wij het logboek zelf en rapporteren wij een bevinding over het systeem, zonder een zorgmedewerker te noemen.

5. Ondersteuning en implementatie. Alleen de documenten die de organisatie ons vraagt in te zien, onder de termijn van de verwerking waar het bij hoort; een gesprek alleen zoals ‘Gesprekken van medewerkers’ beschrijft, ook bij een wettelijke vordering. Wij maken geen kopieën buiten haar omgeving.

6. Dienstmetingen. Aantallen vragen en responstijden per gebruiker, zonder inhoud en zonder namen, alleen om de eigen omgeving van de organisatie te beheren en problemen daarin te verhelpen. Per gebruiker bewaren wij ze 30 dagen, daarna alleen opgeteld per team van minstens vijf mensen. De organisatie krijgt ze nooit per medewerker.

7. Bekwaamheidsdossier. Het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG), voor voorbehouden en risicovolle handelingen volgens het scholingsbeleid van de organisatie. Het legt per medewerker alleen vast welke handeling is uitgevoerd, volgens welk protocol en welke versie, op welke datum en in wiens opdracht, welke beoordelaar de praktijktoets heeft afgetekend, hoelang de bekwaamheid geldig is en wanneer herbeoordeling nodig is, nooit de inhoud van een gesprek, een score of een gebruikscijfer. De bekwaamheid vervalt als de zorgmedewerker de handeling langere tijd niet uitvoert. Het is het dossier van de organisatie; wij houden het in Inora bij als verwerker, op haar instructie, zoals ‘Gesprekken van medewerkers’ beschrijft.

8. Toetsset. Vragen uit de organisatie, en antwoorden die een medewerker of een controle markeerde met hun vraag, ontdaan van namen van cliënten en medewerkers. Wij bewaren ze alleen op schriftelijke opdracht van de organisatie, na instemming van de ondernemingsraad waar zij er een heeft, om elke nieuwe versie van Inora te toetsen voordat die live gaat, en voor niets anders: niet om modellen te trainen en niet voor een andere organisatie. Namen haalt hetzelfde taalmodel in de EU eruit dat de antwoorden geeft; geen mens leest daarvoor een gesprek, en geen medewerker van Axiomatic leest een vraag of antwoord uit de toetsset: de toets van een nieuwe versie is geautomatiseerd. Wij bewaren ze tot de organisatie de opdracht intrekt, uiterlijk tot het einde van de overeenkomst, en verwijderen ze daarna binnen 30 dagen.

9. Antwoordverslag. Van elk antwoord legt Inora vast waarop het rustte: de bronnen met hun versies, de toets die het doorstond en de datum, en een kenmerk dat de medewerker bij het antwoord ziet. Wie vroeg, het tijdstip, de afdeling, de vraag en het antwoord staan er niet in. Het verslag blijft bij ons, nooit bij de organisatie; zij krijgt het alleen op schriftelijk verzoek, voor een incident of een klacht, en nooit wie vroeg.

10. Gebruiksonderzoek. Axiomatic verwerkt geanonimiseerde gebruiksgegevens van Inora voor eigen onderzoek en is daarvoor zelf verwerkingsverantwoordelijke.

11. Dossiergegevens. Zodra Inora het dossier leest, via een koppeling of de eigen login, leest Inora uit het ECD wat de taak die loopt nodig heeft, met de rechten van wie het werk doet: een vraag, de voorbereiding van een bezoek, een evaluatie, een regel of signaal, ook ’s nachts. Een tweede dossier houdt Inora niet bij.

12. Dossierlogboek. Zodra Inora het dossier leest, via een koppeling of de eigen login, legt Inora per stap vast wat het deed, namens wie, voor welke cliënt en met welk resultaat, ingericht volgens NEN 7513. De functie die de organisatie aanwijst, ziet het alleen op schriftelijk verzoek, per cliënt of bij een onderzoek. Wat iemand vraagt, staat er nooit in.

Vragen, antwoorden en rapportages kunnen gegevens over cliënten bevatten, ook over hun gezondheid. De AVG rekent gezondheidsgegevens tot de bijzondere persoonsgegevens. Inora houdt geen tweede cliëntdossier bij en vraagt niet om een burgerservicenummer. Wij behandelen alles wat gebruikers in Inora typen als gezondheidsgegevens, en beveiligen het ook zo.

De organisatie moet voor elke verwerking een grondslag uit artikel 6 AVG vaststellen. Voor gezondheidsgegevens is daarnaast een uitzondering op het verbod uit artikel 9 AVG nodig. Voor noodzakelijke verwerking bij behandeling, verzorging of het beheer van een zorginstelling kan artikel 9, lid 2, onder h AVG, samen met artikel 30, lid 3, onder a van de Uitvoeringswet AVG (UAVG), van toepassing zijn. Dat geldt niet automatisch voor elk gebruik van Inora. De organisatie beoordeelt de noodzaak, de grondslag en het beroepsgeheim voordat

zij zulke gegevens laat verwerken. Artikel 9, lid 3 AVG en artikel 30, lid 4 UAVG stellen eisen aan de geheimhouding. Daarom heeft iedereen bij Axiomatic een geheimhoudingsverklaring getekend.

Wat wij met deze gegevens doen: alleen wat in de verwerkersovereenkomst en in de instructies van de organisatie staat. Wat wij er niet mee doen:

- Wij gebruiken ze niet voor eigen doeleinden, behalve de anonieme aantallen van het gebruiksonderzoek, waarvoor wij zelf verwerkingsverantwoordelijke zijn.
- Wij gebruiken ze niet om modellen te trainen of bij te trainen, en onze modelleverancier ook niet.
- Wij verkopen ze niet en delen ze niet met andere klanten. Verstrekking aan subverwerkers of overheidsinstanties is beperkt tot de gevallen hieronder.
- Wij voegen de gegevens van de ene organisatie niet samen met die van een andere. Elke organisatie heeft een eigen omgeving. Alleen de anonieme aantallen uit het gebruiksonderzoek tellen wij op over ten minste vijf organisaties.
- Wij bekijken de inhoud van gesprekken en documenten niet, behalve in de gevallen onder ‘Wanneer wij gegevens inzien of verstrekken’.

De dienstmetingen bevatten geen inhoud van documenten, vragen of antwoorden en geen namen. Dat maakt ze niet vanzelf anoniem: ook zonder naam kan een meting tot een persoon te herleiden zijn. Daarom behandelen wij ze als persoonsgegevens onder de verwerkersovereenkomst. Wij gebruiken ze niet voor eigen doeleinden of voor het vergelijken van organisaties.

Gesprekken van medewerkers

Wat een medewerker aan Inora vraagt, leest niemand in de organisatie; Axiomatic alleen langs de regels hieronder. Voor de organisatie waar de medewerker werkt, en voor ons, geldt:

- **Niemand in de organisatie leest een gesprek mee, ook de leiding niet.** Geen beheerder, leidinggevende of bestuurder kan in Inora de vragen en antwoorden van een medewerker openen.

- **Verslagen gaan over teams van minstens vijf mensen.** Het maandverslag toont per team de onderwerpen waarover gevraagd wordt en de onderwerpen die nog geen antwoord kregen, met een aantal, nooit een vraag zoals iemand haar typte en nooit per medewerker. Per team gaat het naar de teamleider en de ondernemingsraad; bestuur en kwaliteit krijgen de som over alle teams. Een team van minder dan vijf mensen krijgt geen eigen verslag. Inora beoordeelt niemand en geeft niemand een score.
- **Een vraag zonder antwoord gaat als onderwerp naar de eigenaar.** Staat het antwoord niet in de bronnen, dan krijgt wie over het onderwerp gaat het onderwerp, herschreven zonder herkenbare details en zonder de woorden van wie vroeg, met het aantal keer dat het gevraagd werd, per protocol en opgeteld over alle teams, zodat de bron kan worden aangevuld. De naam van wie vroeg, gaat niet mee.
- **Wij lezen een gesprek alleen in op schriftelijk verzoek, voor een genoemd doel.** Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die de organisatie aanwijst, voor een incident of een klacht; elke inzage wordt vastgelegd en de medewerker hoort ervan. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Wie het verzoek deed, krijgt een bevinding over Inora, nooit wat de medewerker vroeg of las. De functie staat in de verwerkersovereenkomst, zoals de functionaris gegevensbescherming, en wij lezen alleen wat voor het doel nodig is.

Wat een zorgmedewerker Inora vraagt, komt nooit bij de organisatie. Bij de organisatie komt alleen wat de zorgmedewerker zelf verstuurt, zoals een rapportage of een MIC-melding, en het bekwaamheidsdossier dat de inspectie verwacht (Wkkgz, Wet BIG). Dat dossier gaat over voorbehouden en risicovolle handelingen volgens het scholingsbeleid van de organisatie, en het is het dossier van de organisatie zelf. Het legt alleen de handeling, het protocol met zijn versie, de datum en in wiens opdracht vast, nooit de inhoud van een gesprek, een score of een gebruikscijfer, en artikel 5.6 van de verwerkersovereenkomst bindt het. De medewerker ziet het eigen bekwaamheidsdossier altijd in Inora en kan om een kopie vragen om mee te nemen: dat is het recht op inzage (artikel 15 AVG), dat de organisatie beantwoordt en waarbij wij helpen. Een melding die de medewerker zelf bij de MIC-commissie doet, komt daar aan zoals die is verstuurd. Voor de functionaris gegevensbescherming staat alles bij elkaar op Privacy en gegevensbescherming, voor de ondernemingsraad op Ondernemingsraad.

Kunstmatige intelligentie

Stelt een gebruiker een vraag, dan zoekt Inora in de bronnen die de organisatie heeft aangewezen naar de passages die erover gaan. Een taalmodel schrijft daarna een antwoord op basis van die passages. In het antwoord is elke bron van de organisatie gemarkeerd, en één

tik toont de passage. Staat het antwoord niet in de bronnen, dan zegt Inora dat. Zo is elk antwoord controleerbaar: de medewerker ziet waar het vandaan komt en controleert het zelf.

Standaard draait het taalmodel in Amazon Bedrock van Amazon Web Services, via het EU-inferentieprofiel, dat gegevens alleen in regio's binnen de Europese Unie verwerkt. Voor het antwoord verwerkt de dienst de vraag en de gevonden passages. Bij het doorzoekbaar maken van documenten verwerkt een embeddingmodel ook documentpassages; de numerieke representaties daarvan worden in de zoekindex van de organisatie opgeslagen. Amazon Web Services gebruikt deze gegevens niet om modellen te trainen. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model.

Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU. Geen mens leest mee, en het model bewaart niets.

Het systeem kiest per taak het taalmodel, via Amazon Bedrock of via Azure OpenAI van Microsoft Ireland Operations Limited, in een EU-regio. Azure OpenAI draait Axiomatic met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (Microsoft over misbruikmonitoring). Ook Microsoft gebruikt deze gegevens niet om modellen te trainen.

Axiomatic gebruikt gegevens van organisaties niet om modellen te trainen of bij te trainen.

Inora ondersteunt professionals met de kennis van hun organisatie. Het stelt geen diagnose en beslist niet over een behandeling; de professional beslist. Door zijn beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.

Intern gebruiken wij AI-hulpmiddelen bij het schrijven van software. Die hulpmiddelen krijgen geen gegevens van zorgorganisaties.

Wanneer wij gegevens inzien of verstrekken

Om Inora te leveren. Wij werken met zo min mogelijk subverwerkers. Voor de hosting en het taalmodel zijn dat Amazon Web Services en Microsoft Ireland Operations Limited (Azure OpenAI, in een EU-regio). Wie wat verwerkt en waar, staat op Subverwerkers. Elke subverwerker heeft een overeenkomst getekend met verplichtingen die niet lichter zijn dan de onze. Een nieuwe subverwerker melden wij onze klanten 30 dagen voordat hij gegevens gaat verwerken. Een klant kan bezwaar maken.

Voor ons eigen werk. Amazon Web Services host de website en de AI-scan. Google Workspace verzorgt onze e-mail en documenten; meldingen die wij per e-mail sturen, noemen de soorten gegevens en het aantal betrokkenen, nooit gegevens uit Inora. PostHog meet het gebruik van de website en neemt bezoeken op, zoals ‘De website’ beschrijft. Deze diensten krijgen nooit gegevens uit Inora.

Op schriftelijk verzoek van de organisatie. Wij bekijken de inhoud van een gesprek alleen zoals ‘Gesprekken van medewerkers’ beschrijft: op schriftelijk verzoek van de functie die de organisatie daarvoor aanwijst, voor een incident of een klacht. Elke inzage leggen wij vast, en de medewerker hoort ervan. Wat de medewerker vroeg of las, verstrekken wij de organisatie niet. Langs dezelfde weg krijgt de organisatie het antwoordverslag van een antwoord, nooit wie vroeg.

Bij een incident. Bij een beveiligingsincident of een storing onderzoeken wij de systeemlogging en het antwoordverslag, en bekijken wij alleen wat nodig is om het op te lossen; een gesprek van een medewerker lezen wij dan niet. Wij laten het de organisatie weten.

Als de wet ons daartoe verplicht. Wij verstrekken gegevens alleen aan een overheidsinstantie als het Unierecht of Nederlands recht ons daartoe verplicht, bijvoorbeeld op grond van een rechterlijk bevel. Wij verstrekken dan niet meer dan nodig. Tenzij de wet het verbiedt, laten wij het de organisatie weten voordat wij iets verstrekken. Tegen verzoeken zonder geldige wettelijke grondslag maken wij bezwaar. Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.

Als Axiomatic wordt overgenomen. Wij informeren klanten voordat hun persoonsgegevens naar een ander bedrijf gaan of onder een ander beleid vallen. Een overname is op zichzelf geen grondslag om gegevens anders te gebruiken.

Waar de gegevens staan

Inora, voor organisaties in de EU. Voor een organisatie in de Europese Unie worden alle gegevens in Inora in de EU verwerkt en opgeslagen. De productieomgeving en de back-ups draaien bij Amazon Web Services in de regio Europa (Ierland). Het taalmodel draait in de EU. Verwerking buiten de EU vereist eerst een schriftelijke wijziging van de afspraken met de organisatie. Voor doorgifte buiten de Europese Economische Ruimte is bovendien een geldige grond uit hoofdstuk V AVG nodig; toestemming van de organisatie alleen is niet genoeg. Dit geldt ook voor toegang op afstand door een ontvanger buiten de EER.

Deze diensten worden geleverd door Amazon Web Services EMEA SARL in Luxemburg en door Microsoft Ireland Operations Limited in Dublin. Hun moederbedrijven, Amazon.com, Inc. en Microsoft Corporation, zijn Amerikaans en staan allebei op de lijst van het EU-VS-kader voor gegevensbescherming (Data Privacy Framework). Opslag in de EU sluit een verzoek van een buitenlandse overheid niet uit. Zonder geldige wettelijke grondslag maken wij bezwaar, en wij laten het de organisatie eerst weten, tenzij de wet dat verbiedt.

Inora, voor organisaties buiten de EU. Werkt een organisatie buiten de Europese Unie met Inora, dan draait haar omgeving in haar eigen land, bij een leverancier en in een regio die haar verwerkersovereenkomst noemt. Gegevens van organisaties in de EU komen daar nooit.

De website en onze e-mail. Amazon, Google, PostHog, Intercom en IPinfo zijn Amerikaanse bedrijven of horen bij een Amerikaans bedrijf. Een verzoek aan de website kan buiten de EU worden afgehandeld, en e-mail die wij versturen en ontvangen kan buiten de EU worden opgeslagen. Wat PostHog over uw bezoek ontvangt, staat in Duitsland; de chat staat bij Intercom in de Verenigde Staten; IPinfo ontvangt het IP-adres in de Verenigde Staten. Amazon.com, Inc., Google LLC, PostHog, Inc. en Intercom, Inc. staan op de lijst van het EU-VS-kader voor gegevensbescherming (Data Privacy Framework); de verwerkersovereenkomsten van PostHog en Intercom voegen de standaardcontractbepalingen van de EU toe. U kunt via privacy@axiomatic.digital vragen welke waarborgen gelden en een kopie daarvan opvragen.

Hoe wij gegevens beveiligen

Gegevens in Inora zijn versleuteld tijdens transport en bij opslag. Elke organisatie heeft een eigen omgeving. Medewerkers loggen in via de eigen single sign-on van hun organisatie. Alleen de engineers die Inora bouwen en beheren, bij naam in de verwerkersovereenkomst, hebben toegang tot de productieomgeving, met een persoonlijk account en multifactorauthenticatie, en elke toegang wordt vastgelegd. De adviseurs van Axiomatic hebben geen toegang tot gegevens van organisaties. De maatregelen staan op Beveiliging.

Bij een datalek in gegevens waarvoor wij zelf verwerkingsverantwoordelijke zijn, beoordelen wij de meldplichten uit de artikelen 33 en 34 AVG. Wij melden zonder onredelijke vertraging en, waar mogelijk, binnen 72 uur na kennisname bij de Autoriteit Persoonsgegevens, tenzij een risico voor de rechten en vrijheden van mensen onwaarschijnlijk is. Bij een waarschijnlijk hoog risico informeren wij de betrokkenen zonder onredelijke vertraging, tenzij een uitzondering uit artikel 34, lid 3 AVG geldt. Wij leggen elk datalek vast. Voor Inora melden wij het aan de organisatie, zoals Beveiliging beschrijft.

Bewaren en verwijderen

Gesprekken in Inora (vragen, antwoorden en opgestelde rapportages) worden standaard 90 dagen bewaard en daarna verwijderd. De organisatie kan een kortere of langere termijn instellen. Vraagt de functie die de organisatie daarvoor aanwijst binnen de bewaartermijn om een gesprek voor een incident of een klacht, dan houdt Axiomatic het vast tot het onderzoek is afgerond, verwijdert het daarna binnen 30 dagen, en de medewerker hoort ervan.

Documenten blijven in Inora zolang de organisatie ze daar laat staan. Haalt de organisatie een document weg, dan gebruikt Inora het direct niet meer. Kopieën in back-ups zijn binnen 30 dagen weg.

Gebruikersaccounts worden bewaard zolang een gebruiker toegang heeft en tot 30 dagen daarna.

Loggegevens worden 12 maanden bewaard, tenzij de overeenkomst eerder eindigt.

Dienstmetingen worden per gebruiker 30 dagen bewaard, daarna alleen opgeteld per team van minstens vijf mensen.

Het bekwaamheidsdossier staat in Inora zolang de medewerker bij de organisatie werkt, plus 30 dagen; in die 30 dagen exporteert de organisatie het naar haar eigen personeelsdossier, waar haar eigen termijn geldt.

De toetsset blijft bewaard tot de organisatie de opdracht intrekt, uiterlijk tot het einde van de overeenkomst, en wordt daarna binnen 30 dagen verwijderd.

Het antwoordverslag blijft 2 jaar bij ons en wordt daarna vanzelf verwijderd; uit back-ups binnen 30 dagen.

De indeling naar onderwerp verdwijnt met het gesprek.

Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland).

Eindigt een overeenkomst, dan kiest de organisatie voor teruggave of verwijdering. Tot en met dag 30 houden wij de gegevens beschikbaar voor teruggave, tenzij de organisatie eerder om verwijdering vraagt of bevestigt dat de teruggave is afgerond. Uiterlijk op dag 30 verwijderen wij de gegevens uit de actieve systemen, inclusief loggegevens en zoekindexen. Back-upkopieën verdwijnen uiterlijk op dag 60. Alleen een bewaarplicht uit het Unierecht of Nederlands recht kan een uitzondering rechtvaardigen; wij melden dan welke gegevens, grond en termijn dat betreft, tenzij de wet dat verbiedt. De gegevens blijven beschermd zolang wij ze bewaren. Op verzoek bevestigen wij de verwijdering schriftelijk.

Na verwijdering tijdens de looptijd kunnen gegevens nog maximaal 30 dagen in back-ups staan. Bij herstel passen wij verwijderingen opnieuw toe. Dit geldt ook voor gesprekken, accountgegevens en bijbehorende zoekgegevens.

Voor gegevens waarvoor wij zelf verwerkingsverantwoordelijke zijn, staan de termijnen in ‘In één overzicht’.

Uw rechten

U hebt de volgende rechten voor gegevens waarvoor wij verwerkingsverantwoordelijke zijn, onder de voorwaarden van de AVG. Voor gegevens in Inora behandelt de zorgorganisatie deze verzoeken; wij sturen uw verzoek binnen twee werkdagen naar haar door en helpen haar bij het antwoord.

- **Inzage.** U kunt vragen welke persoonsgegevens wij van u hebben en wat wij ermee doen.
- **Rectificatie.** U kunt vragen onjuiste of onvolledige gegevens te verbeteren.
- **Verwijdering.** U kunt vragen uw gegevens te verwijderen. Dat doen wij als de AVG ons daartoe verplicht. Er zijn uitzonderingen, bijvoorbeeld voor een wettelijke bewaarplicht of voor het onderbouwen van een rechtsvordering.
- **Beperking.** U kunt vragen uw gegevens tijdelijk niet te gebruiken, bijvoorbeeld terwijl wij nagaan of ze kloppen.
- **Overdraagbaarheid.** Verwerken wij gegevens die u ons hebt verstrekt geautomatiseerd, op basis van uw toestemming of van een overeenkomst met u, dan kunt u ze opvragen in een gestructureerde, gangbare en machineleesbare vorm. Waar technisch mogelijk kunt u ze rechtstreeks laten overdragen aan een andere verwerkingsverantwoordelijke.
- **Bezwaar.** Waar wij ons op ons gerechtvaardigd belang baseren, kunt u bezwaar maken. Wij stoppen dan, tenzij wij dwingende gerechtvaardigde gronden aantonen die zwaarder wegen dan uw belangen, rechten en vrijheden, of de verwerking nodig is voor een rechtsvordering.
- **Toestemming intrekken.** Waar wij ons op uw toestemming baseren, kunt u die altijd intrekken. Dat verandert niets aan de rechtmatigheid van de verwerking vóór de intrekking.
- **Geen geautomatiseerde besluiten.** Wij nemen geen besluiten over u die alleen op geautomatiseerde verwerking berusten.

Mail privacy@axiomatic.digital. Wij behandelen uw verzoek in beginsel kosteloos en antwoorden zonder onredelijke vertraging, uiterlijk binnen een maand na ontvangst. Is verlenging vanwege de complexiteit of het aantal verzoeken nodig, dan kan die termijn met

maximaal twee maanden worden verlengd. Wij laten u dat binnen de eerste maand weten, met de reden. Wijzen wij uw verzoek af, dan leggen wij uit waarom en hoe u een klacht kunt indienen of naar de rechter kunt gaan.

Bij redelijke twijfel over uw identiteit vragen wij alleen de extra informatie die nodig is om die te bevestigen. Iemand die namens u optreedt, moet zijn bevoegdheid kunnen aantonen; een ondertekende machtiging is één manier.

Klachten

U kunt rechtstreeks een klacht indienen bij de Autoriteit Persoonsgegevens, via autoriteitpersoonsgegevens.nl of per post: Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag. U hoeft daarvoor niet eerst contact met ons op te nemen. U kunt ook terecht bij de bevoegde toezichthouder in het EU-land waar u gewoonlijk woont of werkt, of waar de vermoedelijke inbreuk plaatsvond.

Wijzigingen en vragen

Wij passen deze verklaring aan als de wet, onze diensten of onze subverwerkers veranderen. De datum bovenaan toont de laatste versie. De contactpersonen van onze klanten mailen wij 30 dagen voordat een wezenlijke wijziging ingaat.

Vragen over deze verklaring, uw gegevens of uw rechten: privacy@axiomatic.digital.

AXIOMATIC

Een kwetsbaarheid melden

Vindt u een zwakke plek in Inora, op axiomatic.digital of in de infrastructuur die wij beheren, meld die dan bij ons. Wij bevestigen elke melding en houden u op de hoogte tot het lek dicht is.

Bijgewerkt op 9 november 2026

Waarom dit zwaar weegt

Zorgorganisaties zetten hun protocollen, werkafspraken en kwaliteitshandboek in Inora. Hun medewerkers typen er vragen en rapportages in die over cliënten kunnen gaan, en dus gezondheidsgegevens kunnen bevatten. Een zwakke plek in Inora raakt daarom niet alleen ons, maar ook zorgorganisaties, hun medewerkers en hun cliënten. Wij horen het liever van u dan van iemand die er misbruik van maakt.

Hoe wij Inora en die gegevens beschermen, staat op de pagina Beveiliging.

Wat onder dit beleid valt

- De webapplicatie van Inora, waarin medewerkers van zorgorganisaties vragen stellen en rapporteren.
- De API’s van Inora.
- Deze website, axiomatic.digital.
- De infrastructuur die Axiomatic zelf beheert voor Inora en voor deze website.

Wat er niet onder valt

- Diensten en koppelingen van anderen, zoals de identiteitsdienst van een zorgorganisatie (bijvoorbeeld Microsoft Entra ID) of haar elektronisch cliëntdossier. Meld een kwetsbaarheid daarin bij die organisatie of bij de maker. Raakt die ook Inora, laat het ons dan ook weten.
- Social engineering en phishing van medewerkers van Axiomatic of van zorgorganisaties.
- Aanvallen die de dienst overbelasten of platleggen (DoS en DDoS).

- Geautomatiseerd scannen of testen dat de dienst voor anderen trager of onbereikbaar maakt.
- Fysieke aanvallen op kantoren of datacenters.
- Software en systemen die niet van Axiomatic zijn.

Hoe u meldt

Mail security@axiomatic.digital met ‘Beveiliging’ in de onderwerpregel.

Vermeld in uw melding:

- wat de kwetsbaarheid is en wat iemand ermee zou kunnen;
- de stappen om haar na te bootsen;
- wat het laat zien, zoals schermafbeeldingen, een proof of concept of verzoeken en antwoorden;
- hoe wij u kunnen bereiken voor vragen.

Stuur geen gegevens van anderen mee die u bent tegengekomen. Beschrijf wat u zag, niet de gegevens zelf.

Het adres en dit beleid staan ook in security.txt op axiomatic.digital, volgens RFC 9116.

Wat wij doen, en wanneer

- **Ontvangst.** Wij bevestigen uw melding binnen drie werkdagen.
- **Beoordeling.** Wij onderzoeken de melding, bepalen de ernst volgens de klassen hieronder en laten u weten wat wij vinden.
- **Herstel.** Wij dichten een kritieke kwetsbaarheid binnen 72 uur en andere binnen 30 dagen. Lukt dat niet, dan zeggen wij u waarom en wanneer wel.
- **Op de hoogte.** Tot het lek gedicht is, houden wij u op de hoogte van de voortgang.
- **Zorgorganisaties.** Zijn door de kwetsbaarheid gegevens van een zorgorganisatie ingezien, gewijzigd of verloren gegaan, dan melden wij dat aan die organisatie zonder onredelijke vertraging, uiterlijk 24 uur nadat wij het weten, zoals de pagina Beveiliging beschrijft.
- **Erkenning.** Met uw toestemming noemen wij uw naam zodra het lek gedicht is.

Wat wij van u vragen

- Zie geen gegevens in die niet van u zijn, en wijzig of verwijder ze niet.
- Komt u gegevens van een zorgorganisatie, een medewerker of een cliënt tegen, stop dan meteen, meld het ons en bewaar er geen kopie van.
- Verstoor de dienst niet. Er wordt ook ’s nachts mee gewerkt, als er geen collega is om op terug te vallen.
- Test alleen met accounts die van u zijn of waarvoor u uitdrukkelijk toestemming hebt. Inora kent geen openbare aanmelding: elk account maakt een zorgorganisatie aan, via haar eigen inlog. Wilt u Inora zelf testen, vraag ons dan om toegang.
- Gebruik een kwetsbaarheid niet verder dan nodig is om haar aan te tonen.
- Maak niets openbaar voordat het lek gedicht is, en geef ons daarvoor 90 dagen na uw melding. Is het eerder gedicht, dan spreken wij samen af wanneer u publiceert.
- Doe niets wat verder gaat dan dit beleid toestaat.

Wat wij u toezeggen

Houdt u zich aan dit beleid en handelt u te goeder trouw, dan doen wij geen aangifte en stellen wij geen vordering tegen u in. Spreekt een ander u erop aan, dan verklaren wij dat u binnen dit beleid handelde. Namens anderen, zoals het Openbaar Ministerie of een zorgorganisatie, kunnen wij niet van stappen afzien.

Wij behandelen uw melding en uw gegevens vertrouwelijk, en delen uw naam alleen met uw toestemming.

Hoe wij de ernst bepalen

Klasse	Voorbeelden
Kritiek	Code op afstand uitvoeren; het inloggen omzeilen; toegang tot de omgeving van een andere organisatie; op grote schaal gesprekken, rapportages of documenten inzien; sleutels of geheimen buitmaken.

Klasse	Voorbeelden
Hoog	Binnen een organisatie meer rechten krijgen dan het eigen account geeft; de gesprekken van een andere medewerker inzien; opgeslagen cross-site scripting; SQL- of commando-injectie; Inora laten antwoorden buiten de bronnen van de organisatie of laten oordelen over een cliënt.
Middel	Cross-site request forgery; gegevens zonder gevoelige inhoud die uitlekken; fouten in toegangsrechten met beperkte gevolgen.
Laag	Te uitgebreide foutmeldingen, ontbrekende beveiligingsheaders en andere afwijkingen van goede praktijk met weinig gevolgen.

Wij kijken naar wat een aanvaller in de praktijk kan bereiken, niet alleen naar het type fout. Gaat het om gegevens van cliënten, dan wegen wij de melding zwaarder.