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.