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.