BIJLAGE AI-CARES PRAKTIJKGIDS



AI Data Readiness Checklist

Is je organisatie en haar data klaar voor AI?
14 september 2026

Waarom deze checklist?

AI biedt veel kansen voor organisaties in welzijn en zorg: AI kan helpen om administratieve taken te verlichten, processen efficiënter te organiseren, patronen in data te herkennen of de kwaliteit van ondersteuning en dienstverlening te versterken. Maar het verantwoord gebruik van AI begint niet enkel bij de technologie. Het begint bij data, mensen, afspraken en verantwoordelijkheden.

Voor je als organisatie met AI aan de slag gaat, moet je zicht krijgen op enkele **basisvragen**:

- ✓ Welke gegevens hebben we?
- ✓ Waar zitten die gegevens?
- ✓ Zijn ze bruikbaar en voldoende betrouwbaar?
- ✓ Mogen we ze gebruiken voor het doel dat we voor ogen hebben?
- ✓ Wie is verantwoordelijk?
- ✓ Wie waakt over privacy en gegevensbescherming?
- ✓ Welke afspraken zijn nodig als we samenwerken met een externe partner?

Die vragen zijn extra belangrijk wanneer je werkt met **persoonsgegevens**. In welzijn en zorg gaat het vaak over mensen in kwetsbare situaties. Soms gaat het ook om bijzondere categorieën van

persoonsgegevens, zoals gezondheidsgegevens of gegevens over psychisch welzijn. Onzorgvuldig gebruik van die data kan gevolgen hebben voor hun privacy, vertrouwen, rechten en veiligheid.

Deze checklist helpt je organisatie om stap voor stap na te gaan of de basisvoorwaarden aanwezig zijn om verantwoord met data en AI aan de slag te gaan. De focus ligt niet op de AI-technologie zelf, maar op wat nodig is vóór je een AI-project opstart:

1. duidelijke rollen en verantwoordelijkheden;
2. zicht op welke data beschikbaar is, waar die data zit en in welke vorm;
3. duidelijkheid over wat juridisch mag en onder welke voorwaarden;
4. aandacht voor anonimisering, pseudonimisering en bescherming van betrokkenen;
5. goede afspraken wanneer data gedeeld wordt met externe partners.

Het doel is niet om alle vragen meteen perfect te beantwoorden. De checklist helpt vooral om in kaart te brengen waar je organisatie vandaag staat, welke blinde vlekken er nog zijn en welke eerste acties nodig zijn. Gebruik ze dus als praktische gids en als vertrekpunt voor gesprek binnen je organisatie.

Disclaimer
Deze checklist is opgesteld als informatief en praktisch hulpmiddel, op basis van de inzichten en informatie die beschikbaar waren op het moment van opmaak. Hoewel de inhoud met zorg is samengesteld, kan niet worden gegarandeerd dat de checklist volledig of toepasbaar is op elke concrete situatie. Ze vervangt geen juridisch advies en ook geen beoordeling door je DPO, jurist of privacy-verantwoordelijke. De auteurs kunnen niet aansprakelijk worden gesteld voor het gebruik van deze checklist of de beslissingen die op basis van deze informatie worden genomen.

Het blijft de verantwoordelijkheid van de organisatie om na te gaan of een AI-piste juridisch, ethisch, technisch en organisatorisch verantwoord is, en om hierover tijdig de juiste interne of externe expertise te betrekken.

Voor wie is deze checklist?

Deze checklist is bedoeld voor organisaties binnen welzijn en zorg die met persoonsgegevens werken. Vaak gaat het daarbij ook om gevoelige gegevens, zoals informatie over gezondheid, psychisch welzijn, hulpvragen, gezinssituaties of andere persoonlijke omstandigheden van cliënten, gebruikers, patiënten of burgers.

De checklist is bedoeld voor organisaties die AI of datagedreven toepassingen willen verkennen, voorbereiden of op een verantwoorde manier willen inzetten. Ze helpt om vooraf beter zicht te krijgen op de data, rollen, afspraken en randvoorwaarden die daarvoor nodig zijn. De checklist richt zich niet op één specifieke functie binnen deze organisaties. Ze is bedoeld voor iedereen die betrokken is bij digitale innovatie met AI, zoals:

- directie- en beleidsmedewerkers
- projectverantwoordelijken
- data stewards of dataverantwoordelijken
- IT-medewerkers
- kwaliteitszorgmedewerkers
- privacyverantwoordelijken

- innovatiemedewerkers.

Je hoeft geen juridische, technische of AI-expert te zijn om met deze checklist aan de slag te gaan. De checklist is net bedoeld als laagdrempelig startpunt om het gesprek binnen je organisatie op gang te brengen. Ze helpt om verschillende perspectieven samen te brengen: praktijk, beleid, IT, data, privacy en innovatie.

De checklist geeft geen definitief juridisch oordeel. Ze helpt wel om beter voorbereid in gesprek te gaan met je DPO, jurist of privacyverantwoordelijke.

Hoe gebruik je deze checklist?

Deze checklist helpt je organisatie om na te gaan of de basisvoorwaarden aanwezig zijn om verantwoord met data en AI aan de slag te gaan. Vertrek vanuit een concrete nood, vraag of verbeterkans in je organisatie. Welk proces loopt vandaag moeilijk? Welke taak vraagt veel tijd? Welke informatie ontbreekt? Waar botsen medewerkers, cliënten, patiënten, burgers of gebruikers op terugkerende problemen?

Deze checklist helpt je om gericht te onderzoeken of je organisatie klaar is om de piste van AI verantwoord te verkennen en bestaat uit vijf thema's die samen een stevige basis vormen voor verantwoord datagebruik en AI-toepassingen:

1. **Rollen**: Wie moet betrokken worden en wie neemt welke verantwoordelijkheid op?
2. **Data:** Welke gegevens zijn beschikbaar, waar zitten ze, in welke vorm bestaan ze en zijn ze bruikbaar?
3. **Juridische voorwaarden:** Mogen we deze data gebruiken voor het doel dat we voor ogen hebben, en onder welke voorwaarden**?**
4. **Anonimisering en pseudonimisering:** Hoe beschermen we de mensen achter de data en hoe beperken we het risico op herkenbaarheid?
5. **Data delen:** Welke afspraken zijn nodig wanneer data gedeeld wordt met externe partners, zoals onderzoekers, ontwikkelaars of technologiepartners?

Voor je de checklist invult, omschrijf je kort de AI-piste die je wil verkennen. Bijvoorbeeld: *chatgesprekken analyseren om terugkerende hulpvragen beter te begrijpen*.

Wat willen we met AI doen?
We willen nagaan of AI kan helpen om patronen te herkennen in chatgesprekken met cliënten. Bijvoorbeeld: welke thema's komen vaak terug, welke vragen worden vaak gesteld, op welke momenten zoeken cliënten hulp, en welke noden worden mogelijk nog onvoldoende opgevangen?

Voor wie is de toepassing bedoeld?
De toepassing is in eerste instantie bedoeld voor de organisatie zelf: beleidsmedewerkers, coördinatoren, kwaliteitsmedewerkers en praktijkmedewerkers die de dienstverlening willen verbeteren. De toepassing is niet bedoeld om individuele cliënten te beoordelen of automatisch beslissingen over hen te nemen.

Welke meerwaarde verwachten we?

We verwachten beter zicht te krijgen op terugkerende hulpvragen en mogelijke hiaten in het aanbod.

Breng collega's samen die elk vanuit hun eigen expertise naar de vragen in deze checklist kijken: praktijk, beleid, IT, data, privacy, kwaliteit en innovatie. De meerwaarde zit niet alleen in het invullen van de vragen, maar vooral in het gesprek dat erdoor ontstaat.

Vanuit je concrete AI-piste kan je stap voor stap nagaan welke data nodig is, wie betrokken moet worden, wat juridisch moet worden afgetoetst en welke afspraken nodig zijn. Zo wordt zichtbaar waar je vandaag staat, welke vragen al beantwoord zijn, waar nog blinde vlekken zitten en welke acties nodig zijn voor je verdergaat.

Vraag 1: Bij wie moet je zijn? DE ROLLEN

AI-projecten waarbij je data gebruikt, vragen meer dan goede technologie. Je moet ook weten wie betrokken moet worden en wie waarvoor verantwoordelijk is. Wie kent de data? Wie begrijpt de praktijk waaruit de data komt? Wie waakt over privacy en gegevensbescherming? Wie kent de technische systemen? Wie kent de afspraken met leveranciers, partners of platformen? En wie heeft het mandaat om beslissingen te nemen over datagebruik, samenwerking of risico's?

DPO, jurist of andere bevoegde persoon
Ga eerst na of je organisatie een DPO heeft. Een DPO, of *Data Protection Officer*, waakt mee over gegevensbescherming en geeft advies over privacy, GDPR, rechtsgrond, datadeling en risico's voor betrokkenen. Een DPO heeft een onafhankelijke advies- en controlefunctie. De DPO denkt dus mee, maar neemt niet zomaar de operationele beslissingen over een AI-project. Niet elke organisatie is verplicht om een DPO aan te stellen. Ook als je organisatie geen formele DPO heeft, is het belangrijk om te weten wie intern of extern aanspreekbaar is voor vragen over privacy en gegevensbescherming. Dat kan bijvoorbeeld een jurist, privacyverantwoordelijke of externe adviseur zijn.

Let op: niet alle juridische vragen zijn automatisch DPO-vragen. Als het gaat over gebruiksrechten, licenties, contracten met leveranciers of samenwerkingsovereenkomsten, moet je ook weten wie daarover kan meekijken. Dat kan een jurist zijn, maar ook iemand van aankoop, contractbeheer, beleid of projectcoördinatie.

Data steward
Daarnaast is het zinvol om een data steward of brugfiguur aan te duiden. Dat is iemand die het overzicht helpt bewaren: deze persoon begrijpt de noden op de werkvloer, maar kan evengoed in gesprek gaan met IT, beleid, juridisch verantwoordelijken en externe partners. Daardoor heeft deze rol een grote impact op de haalbaarheid van datagedreven projecten.

Deze persoon hoeft geen dataspecialist te zijn, maar begrijpt voldoende hoe de organisatie werkt, waar data ontstaat, wie ermee werkt en welke vragen er leven op de werkvloer. De data steward helpt om de juiste mensen samen te brengen en voorkomt dat data- en AI-vragen alleen bij IT of beleid terechtkomen. Ook wanneer je een DPO hebt, is een datasteward erg zinvol, vanwege de toegankelijkheid en praktijkgerichtheid.

Databeheerder
Er is ook iemand nodig die de technische kant kent. Meestal gaat dit om iemand met IT-vaardigheden, een databeheerder. Deze persoon weet bijvoorbeeld:

- in welke systemen data wordt opgeslagen;
- wie toegang heeft;
- of data veilig geëxporteerd kan worden;
- welke technische beperkingen er zijn;
- wat er moet gebeuren als er een technisch probleem of beveiligingsincident is.

Beslissingsnemer met mandaat
Tot slot moet duidelijk zijn wie beslissingen mag nemen. AI-projecten vragen keuzes over prioriteiten, middelen, samenwerking, risico's en verantwoordelijkheid. Zorg dus dat je weet wie het mandaat heeft om te beslissen of een AI-project wordt opgestart, aangepast, stopgezet of voorgelegd aan de juiste interne of externe experten.

CHECKLIST

- ☐ We weten we wie intern of extern aanspreekbaar is met vragen rond privacy en gegevensbescherming. We weten of onze organisatie een DPO heeft en hoe we die persoon kunnen bereiken.
- ☐ We weten wie kan meekijken naar contracten, licenties, gebruiksvoorwaarden of afspraken met leveranciers en partners.
- ☐ We weten wie de brug kan maken tussen de noden uit de praktijk, IT, beleid, en privacy (data steward).
- ☐ We weten wie technisch overzicht heeft over onze systemen, databanken, platformen, toegang en exports. We weten wie we moeten contacteren als er iets misloopt met data, toegang, beveiliging of datadeling (databeheerder)
- ☐ We weten wie het mandaat heeft om beslissingen te nemen over datagebruik, AI-toepassingen of samenwerking met externe partners (beslissingsnemer).
- ☐ We hebben de namen, rollen en contactgegevens van deze personen op één plaats verzameld.

Eerste stap
Kan je nog niet alle vragen afvinken? Dan kan je hiermee aan de slag: ofwel is er nog niemand aangeduid voor een bepaalde rol, ofwel is niet voor iedereen duidelijk wie deze rol opneemt.

Maak een eenvoudig rollenoverzicht. Noteer minstens:

1. Wie kijkt mee naar privacy en gegevensbescherming?
2. Wie kent de contracten, licenties of afspraken met leveranciers, partners of data-aanbieders het best?
3. Wie kent onze systemen en data technisch het best?
4. Wie begrijpt de betekenis van data in de praktijk?
5. Wie bewaart het overzicht en brengt de juiste mensen samen?
6. Wie mag beslissen of we met een AI-project, data-uitwisseling of een externe partner verdergaan?

Vraag 2: Welke data hebben we, waar zit ze en in welke vorm? DE DATA

Voor je met AI aan de slag kan, moet je weten welke data je organisatie heeft. Data omvat meer dan je misschien denkt: het kan gaan over chatgesprekken, cliëntverslagen, registraties, handleidingen, interne documenten, rapporten,... Daarom is een overzicht essentieel: waar zit de data? In welk systeem of platform wordt ze bewaard? Wie heeft toegang? Kan je de data exporteren? En in welke vorm komt ze eruit?

Niet alle data is meteen bruikbaar voor AI. Soms zit data vast in een systeem. Soms kan je ze alleen downloaden als pdf, terwijl je eigenlijk tekst of tabelgegevens nodig hebt. Soms is data onvolledig, verschillend genoteerd of moeilijk te interpreteren zonder kennis van de praktijk.

Ook de kwaliteit van de data is belangrijk. In de datawereld wordt vaak gezegd: “garbage in, garbage out”. Als de data onvolledig, rommelig of onduidelijk is, zal ook de output van een AI-toepassing minder betrouwbaar zijn. Controleer dus niet alleen of de data bestaat, maar ook of ze voldoende volledig, consistent en begrijpelijk is voor het doel dat je voor ogen hebt.

In deze stap breng je vooral in kaart welke data er is en of die mogelijk bruikbaar is. Dat betekent niet dat je de data al zomaar mag kopiëren, exporteren, analyseren of delen. Of dat juridisch mag, bekijk je verder in de checklist, samen met je DPO, jurist of privacyverantwoordelijke.

CHECKLIST

- ☐ We weten welke data mogelijk relevant zijn voor onze AI-piste
- ☐ We weten in welke systemen, platformen, documenten of bestanden deze data zit.
- ☐ We weten wie toegang heeft tot deze data.
- ☐ We weten wie de betekenis van deze data in de praktijk goed begrijpt.
- ☐ We weten in welke vorm de data beschikbaar is (bijvoorbeeld als tekst, tabel, pdf, exportbestand, vrije tekst of vaste velden).
- ☐ We weten of de data geëxporteerd kan worden.
- ☐ We weten of de data gestructureerd is (in tabellen, vaste velden) of bestaat uit vrije tekst (zoals e-mails, verslagen, dossiers, chatgesprekken,…)
- ☐ We weten of de data volledig genoeg is voor het doel dat we voor ogen hebben.
- ☐ We weten of dezelfde informatie op een consistente manier wordt genoteerd.
- ☐ Ik weet wie kan helpen als data onvolledig, onduidelijk of moeilijk exporteerbaar is.

Eerste stap

Maak een eenvoudige data-inventaris voor jouw concrete AI-piste. Noteer minstens:

1. Welke informatie hebben we echt nodig voor deze AI-piste?
2. Waar wordt die informatie bewaard?
3. Wie heeft toegang?
4. In welke vorm bestaat de data?
5. Kan de data geëxporteerd worden?
6. Wie begrijpt de betekenis van de data in de praktijk?
7. Welke beperkingen of kwaliteitsproblemen zien we?

Vraag 3: Wat mag en onder welke voorwaarden? DE RECHTSGROND

Als je data wil gebruiken voor AI, onderzoek, kwaliteitsverbetering of samenwerking met een externe partner, moet je nagaan of dat juridisch mag. Goede bedoelingen volstaan niet: je moet kunnen uitleggen waarvoor je de data wil gebruiken, waarom dat nodig is en onder welke voorwaarden dat kan.

Daarbij moet je minstens naar twee zaken kijken. Ten eerste: mag je persoonsgegevens verwerken volgens de regels rond gegevensbescherming? Ten tweede: mag je de data, databank of inhoud ook gebruiken volgens de geldende gebruiksrechten, contracten en licenties?

Je hoeft die juridische beoordeling niet alleen te maken. Daarvoor betrek je je DPO, jurist of privacy-verantwoordelijke. Wat je wel kan doen, is de juiste vragen voorbereiden.

Gegevensbescherming
Een eerste belangrijke vraag is: waarvoor hebben we deze data oorspronkelijk verzameld, en willen we ze nu voor hetzelfde doel of voor iets nieuws gebruiken?

Een gevoerd gesprek met een cliënt, gebruiker, patiënt of burger betekent bijvoorbeeld niet automatisch dat je die gegevens later ook mag gebruiken voor AI of nieuwe technologische ontwikkelingen. Zeker bij cliëntinformatie, hulpvragen of gezondheidsgegevens moet je extra voorzichtig zijn.

Voor elke verwerking van persoonsgegevens heb je een geldige rechtsgrond nodig. Organisaties denken soms: “we vragen toestemming aan de gebruikers”. Dat kan, maar toestemming is maar één mogelijke rechtsgrond. Welke rechtsgrond passend is, hangt af van het doel, de context, de soort data, de relatie met de betrokkene en de wettelijke opdracht van je organisatie.

Als je **toestemming** gebruikt, moet die toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig zijn (‘informed consent’). Betrokkenen moeten dus begrijpen waarvoor hun gegevens gebruikt worden en moeten een echte keuze hebben. Toestemming geven voor hulpverlening is niet automatisch toestemming voor hergebruik van die gegevens in een AI-project.

Ga na wat cliënten, patiënten, gebruikers of burgers al te horen kregen over het gebruik van hun gegevens. Staat in de **privacyverklaring** waarvoor gegevens worden verzameld en gebruikt? Wordt (her)gebruik voor onderzoek, kwaliteitsverbetering of ontwikkeling vermeld? Is duidelijk of gegevens gedeeld kunnen worden met externe partners? En is uitgelegd welke rechten betrokkenen hebben?

Als dat niet duidelijk is, ga dan niet zomaar verder. Verzamel eerst de nodige informatie en leg de vraag voor in het gesprek met je DPO, jurist of privacyverantwoordelijke. Het kan goed zijn dat je de privacyverklaring van je organisatie zult moeten veranderen. Je kan dan enkel data gebruiken dat werd verzameld nadat deze nieuwe privacyverklaring actief werd.

Gebruiksrechten en licenties
Naast gegevensbescherming moet je ook nagaan of je de data of inhoud mag gebruiken volgens de geldende gebruiksrechten, contracten en licenties. Niet alles wat technisch beschikbaar is, mag zomaar worden gekopieerd, geëxporteerd, gedeeld, verrijkt of gebruikt voor AI. Dat speelt

bijvoorbeeld wanneer data afkomstig is uit een extern platform, een commerciële tool of materiaal van een partnerorganisatie. Je moet dus nagaan of er auteursrechten, licentievoorwaarden of contractuele afspraken gelden: wie heeft de rechten op de inhoud, wat staat er in het contract met de leverancier en is export met een externe partner toegelaten?

Gebruiksrechten en licenties gaan dus over een andere vraag dan gegevensbescherming. Bij gegevensbescherming vraag je: mogen we persoonsgegevens verwerken voor dit doel? Bij gebruiksrechten en licenties vraag je: hebben we het recht om deze data, databank of inhoud op deze manier te gebruiken?

Let op: deze checklist helpt om de juiste vragen te stellen, maar neemt de verantwoordelijkheid van de organisatie niet over. De organisatie blijft zelf verantwoordelijk om persoonsgegevens, gevoelige gegevens en AI-toepassingen op een juridisch, GDPR-conform en ethisch verantwoorde manier te gebruiken. Betrek daarom tijdig je DPO, jurist, privacyverantwoordelijke en andere bevoegde personen, zeker wanneer de AI-piste impact kan hebben op cliënten, patiënten of gebruikers.

CHECKLIST

Het oorspronkelijke gebruik

- ☐ We weten waarvoor de data oorspronkelijk verzameld werd.
- ☐ We weten op welke rechtsgrond de data vandaag verwerkt wordt.
- ☐ We weten wat cliënten, patiënten, gebruikers of burgers hierover te lezen kregen in onze privacyverklaring.

Het nieuwe gebruik

- ☐ We weten waarvoor we de data nu willen gebruiken.
- ☐ We hebben nagegaan of dit nieuwe gebruik past bij het oorspronkelijke doel.
- ☐ We hebben nagegaan of voor deze AI-piste een nieuwe of bijkomende juridische beoordeling nodig is.

De soort data

- ☐ We weten of de data persoonsgegevens of gevoelige gegevens bevat, zoals gezondheidsgegevens of gegevens over psychisch welzijn.
- ☐ We weten of de data of inhoud afkomstig is uit een extern platform, een databank, een tool, een vragenlijst, een methodiek of materiaal van een partnerorganisatie.

Informatie aan betrokkenen

- ☐ We hebben gecontroleerd of onze privacyverklaring dit gebruik voldoende duidelijk beschrijft.
- ☐ We hebben gecontroleerd of bestaande consentteksten of informatieformulieren dit gebruik voldoende dekken.

Extern gebruik of delen

- ☐ We weten of de data binnen de organisatie blijft of gedeeld wordt met een externe partner.
- ☐ We weten of een externe partner de data alleen in onze opdracht verwerkt, of ook zelf mee bepaalt wat ermee gebeurt.

Gebruiksrechten en licenties

- ☐ We hebben nagegaan of we de data contractueel mogen gebruiken voor dit nieuwe doel.
- ☐ We hebben de relevante overeenkomsten, licenties of gebruiksvoorwaarden met partners, leveranciers of data-aanbieders nagelezen.

- ☐ We hebben gecontroleerd of hergebruik voor AI, onderzoek of kwaliteitsverbetering toegestaan is.
- ☐ We hebben gecontroleerd of er contractuele beperkingen zijn op kopiëren of exporteren van data, delen van data, combineren of verrijken van data, trainen of testen van AI-modellen, publicatie of commercieel gebruik,…
- ☐ Indien nodig hebben we contractuele afspraken aangepast of uitgebreid vóór gebruik.

DPO check

- ☐ We weten welke vragen we moeten voorleggen aan onze DPO, jurist of privacyverantwoordelijke.
- ☐ We gaan niet verder met gebruiken, exporteren, analyseren of delen van persoonsgegevens zolang niet duidelijk is of dit juridisch mag.
- ☐ We gaan niet verder met gebruiken, exporteren, analyseren of delen van data zolang niet duidelijk is of gebruiksrechten, licenties of contractuele afspraken dit toelaten.
- ☐ We hebben met onze DPO, jurist of privacyverantwoordelijke afgestemd welke verplichtingen uit de Europese AI Act mogelijk relevant zijn voor deze AI-piste.

Eerste stap

Leg je AI-piste naast deze documenten of informatiebronnen:

1. de privacyverklaring;
2. eventuele 'informed consent' teksten of informatieformulieren;
3. het verwerkingsregister;
4. relevante contracten met leveranciers, partners of data-aanbieders

Beantwoord daarna samen met je DPO, jurist, privacyverantwoordelijke of andere bevoegde persoon deze vragen:

- ✓ Waarvoor werd de data oorspronkelijk verzameld?
- ✓ Waarvoor willen we de data nu gebruiken?
- ✓ Weten betrokkenen dat hun data hiervoor gebruikt kan worden?
- ✓ Gaat het om persoonsgegevens of gevoelige gegevens?
- ✓ Mogen we de data volgens contracten, licenties of gebruiksvoorwaarden gebruiken voor dit nieuwe doel?
- ✓ Mag de data gedeeld worden met een externe partner?
- ✓ Mag de data gebruikt worden voor AI, onderzoek, ontwikkeling of kwaliteitsverbetering?
- ✓ Moet onze DPO, jurist, privacyverantwoordelijke of contractverantwoordelijke dit beoordelen voor we verdergaan?

Als het antwoord op één van deze vragen onduidelijk is, ga dan nog niet verder met het gebruiken, exporteren of delen van de data. Breng eerst in kaart wat moet worden aangepast of juridisch nagekeken.

Vraag 4: Hoe beschermen we de mens achter de data? ANONIMISERING/PSEUDONIMISERING

Organisaties in welzijn en zorg werken vaak met gegevens over mensen in kwetsbare situaties. Denk aan cliënten, patiënten, gebruikers of burgers die hulp zoeken, persoonlijke informatie delen of ondersteuning krijgen. Die data gaat dus niet over abstracte cijfertjes, maar over echte mensen. Onzorgvuldig gebruik kan gevolgen hebben voor hun privacy, vertrouwen, rechten en veiligheid.

Daarom moet je nagaan hoe herkenbaar mensen nog zijn in de data die je wil gebruiken. Dat is niet altijd eenvoudig. Ook als je namen, e-mailadressen of telefoonnummers verwijdert, kunnen mensen soms nog herkend worden door details in hun verhaal. Denk aan een woonplaats, school, leeftijd, gezinssituatie, zeldzame gebeurtenis, functie of combinatie van deze kenmerken. Het is voldoende dat het *theoretisch mogelijk* is om een persoon te herkennen door enkele 'puzzelstukjes' samen te leggen, om te concluderen dat volledig anonimiseren niet mogelijk is.

Vrije tekst bevat vaak meer herkenbare informatie dan je op het eerste gezicht ziet. Een cliënt kan bijvoorbeeld geen naam noemen, maar wel verwijzen naar een kleine gemeente, een specifieke school, een bijzondere gezinssituatie of een herkenbare gebeurtenis. Daarom volstaat het meestal niet om alleen namen te verwijderen. Je moet ook kijken naar indirect herkenbare details en naar combinaties van gegevens.

Namen verwijderen is niet hetzelfde als anonimiseren
Veel data lijkt anoniem omdat directe gegevens, zoals naam of contactgegevens, verwijderd zijn. Toch kan iemand nog herkenbaar blijven door andere informatie in de tekst of door de combinatie van verschillende gegevens. Daarom is het belangrijk om het verschil te kennen tussen persoonsgegevens, gepseudonimiseerde data en anonieme data.

- **Persoonsgegevens** zijn gegevens waarmee iemand rechtstreeks of onrechtstreeks herkenbaar is. Dat kan gaan om een naam of e-mailadres, maar ook om een chatgesprek met veel persoonlijke details.
- **Gepseudonimiseerde data** is data waarin herkenbare (persoons)gegevens verwijderd vervangen of afgeschermd zijn (bijvoorbeeld door een code) maar via een sleutelbestand of door combinatie met andere informatie toch nog opnieuw aan een persoon gekoppeld kunnen worden. Gepseudonimiseerde data blijft daarom vallen onder de wettelijke categorie 'persoonsgegevens'.
- **Anonieme data** is data waarbij het redelijkerwijs niet meer mogelijk is om te achterhalen over wie het gaat. Dat is een hoge lat. Zeker bij vrije tekst (zoals chatgesprekken, verslagen of hulpvragen) is volledige anonimisering vaak moeilijk.

Soort data	**Betekenis**	**Voorbeeld**	**Data mag gedeeld worden?**
Persoonsgegevens	Gegevens waarmee iemand direct of indirect herkenbaar is.	Een chatgesprek met naam, e-mailadres, IP-adres of herkenbare persoonlijke details.	Nee
Gepseudonimiseerde gegevens	Herkenbare gegevens zijn vervangen of verwijderd, maar de oorspronkelijke persoonsgegevens kunnen (theoretisch) gereconstrueerd worden met extra informatie, sleutels of context.	Een chatgesprek zonder persoonsnamen, maar wel met leeftijd, woonplaats, school en specifieke thuissituatie. Iemand kan deze persoon herkennen door de puzzelstukjes samen te leggen.	Alleen met de juiste afspraken en maatregelen. Die afspraken worden in een juridische overeenkomst gegoten (*zie verder*)

Anonieme data	Het is niet meer redelijk mogelijk om te achterhalen over wie het gaat.	Loutere totaalcijfers, zoals het aantal gesprekken per maand per thema.	Ja, anonieme data valt niet onder de GDPR-wetgeving

Bescherm ook de sleutel
Bij pseudonimisering wordt soms gewerkt met een sleutelbestand. Dat is een apart bestand waarmee een code opnieuw gekoppeld kan worden aan een persoon. Bijvoorbeeld: “Gebruiker 123” wordt in een apart bestand gekoppeld aan een naam, dossiernummer of andere identificerende informatie. Zo’n sleutelbestand moet strikt gescheiden, veilig en beperkt toegankelijk bewaard worden. Alleen personen die daar een duidelijke reden en bevoegdheid voor hebben, mogen erbij.

De verantwoordelijkheid ligt bij de organisatie
De verantwoordelijkheid om data te beschermen ligt bij de organisatie en haar partners, niet bij de cliënt, patiënt, gebruiker of burger. Je kan dus niet verwachten dat mensen zelf vermijden om persoonsgegevens te delen in een hulpverleningsgesprek.

Beslis daarom niet alleen of data anoniem genoeg is. Betrek je DPO, jurist, privacyverantwoordelijke of een expert in gegevensbescherming, zeker wanneer het gaat om chatgesprekken, cliëntinformatie, gezondheidsgegevens of andere gevoelige gegevens.

CHECKLIST
Herkenbaarheid
- ❑ We weten of de data persoonsgegevens of gevoelige gegevens bevat. We hebben nagegaan of mensen *rechtstreeks* herkenbaar zijn, bijvoorbeeld door naam, e-mailadres, telefoonnummer, dossiernummer, IP-adres,…
- ❑ We hebben nagegaan of mensen *onrechtstreeks* herkenbaar kunnen zijn door details in tekst, context of combinaties van gegevens.

Anonimisering of pseudonimisering
- ❑ We weten welke gegevens niet nodig zijn en daarom verwijderd of afgeschermd moeten worden.
- ❑ We weten of de data echt anoniem kan worden gemaakt of alleen gepseudonimiseerd kan worden.
- ❑ We weten welke persoonsgegevens verwijderd, vervangen of afgeschermd moeten worden vóór de data gebruikt of gedeeld wordt. We weten dat namen verwijderen niet automatisch betekent dat de data anoniem is.
- ❑ We weten of vrije tekst, zoals chatgesprekken, verslagen of hulpvragen, extra controle nodig heeft op herkenbare details.

Toegang en beveiliging
- ❑ We weten wie toegang heeft tot de oorspronkelijke data.
- ❑ We weten wie toegang heeft tot de gepseudonimiseerde of geanonimiseerde data.
- ❑ We weten of er een sleutelbestand bestaat waarmee data opnieuw aan personen gekoppeld kan worden.
- ❑ We hebben afspraken over wie toegang heeft tot dat sleutelbestand en hoe het beveiligd wordt.

DPO-check

- ❑ We hebben met onze DPO, jurist of privacyverantwoordelijke afgestemd of de data voldoende beschermd is voor het beoogde gebruik.
- ❑ We gaan niet verder met gebruiken, analyseren of delen van gevoelige data zolang niet duidelijk is of de bescherming voldoende is.

Eerste stap
Neem enkele voorbeelden van de data die je mogelijk wil gebruiken, bijvoorbeeld een chatgesprek, verslag, registratie of exportbestand. Bekijk samen met iemand uit de praktijk, IT/data en privacy:

- ✓ Welke directe herkenningsgegevens staan erin?
- ✓ Welke indirect herkenbare details staan erin?
- ✓ Welke combinaties van gegevens kunnen iemand herkenbaar maken?
- ✓ Welke gegevens zijn echt nodig voor onze AI-piste?
- ✓ Welke gegevens kunnen we verwijderen, vervangen of afschermen?
- ✓ Is anonimisering realistisch, of gaat het eerder om pseudonimisering?
- ✓ Wie moet dit beoordelen voor we verdergaan?

Vraag 5: Mag ik je data even lenen? DATA DELEN

AI-projecten vragen vaak samenwerking. Je werkt misschien samen met een onderzoekspartner, technologiepartner, softwareontwikkelaar, hogeschool, universiteit of externe leverancier. Zodra een externe partij toegang krijgt tot data, moet duidelijk zijn wat er precies gebeurt. Data delen betekent niet alleen dat je een bestand doorstuurt. Ook toegang geven tot een platform, werken in een gedeelde cloudomgeving, data laten analyseren door een externe partner of een tool laten draaien op jouw data kan betekenen dat persoonsgegevens extern verwerkt worden.

Zeker bij persoonsgegevens, chatgesprekken of andere gevoelige data moet je vooraf duidelijke afspraken maken. Je moet weten welke data gedeeld wordt, met wie, waarom, op welke juridische basis, via welk kanaal, wie toegang krijgt en wat er na afloop met de data gebeurt.

Begin bij rolverdeling
Niet elke externe partner heeft dezelfde rol. Soms verwerkt een externe partij data alleen in opdracht van jouw organisatie. Denk aan een leverancier die een tool beheert of een ontwikkelaar die in jouw opdracht een toepassing bouwt. Dan is een **verwerkersovereenkomst** nodig.

In andere gevallen bepaalt de externe partner zelf mee wat er met de data gebeurt, bijvoorbeeld bij bepaalde vormen van onderzoek of gezamenlijke ontwikkeling. Dan kan een andere overeenkomst nodig zijn, zoals een **samenwerkingsovereenkomst, data sharing agreement** of **data transfer agreement**. Bepaal dit niet zelf. Laat je DPO, jurist of privacyverantwoordelijke beoordelen welke rol elke partij heeft en welke overeenkomst nodig is.

Controleer het verwerkingsregister
Ga ook na of de verwerking in het **verwerkingsregister** staat. Daarin documenteert je organisatie welke persoonsgegevens ze verwerkt, voor welk doel, op basis van welke rechtsgrond, wie toegang heeft, met wie gegevens gedeeld worden en hoe lang ze bewaard worden. Als je data op een nieuwe manier gebruikt, deelt met een externe partner of laat verwerken door een AI-tool, moet je nagaan of het verwerkingsregister moet worden aangevuld of aangepast vóór je start.

Deel alleen wat nodig is
Deel niet meer data dan nodig is voor de AI-piste. Hoe minder gevoelige of herkenbare data je deelt, hoe kleiner het risico. Vraag telkens:

- Welke data heeft de externe partner echt nodig?
- Kan het ook met minder data?
- Kan het met geanonimiseerde of gepseudonimiseerde data?
- Moeten bepaalde velden, teksten of details verwijderd worden?
- Moet de partner toegang krijgen tot de data, of volstaat een beperkte export?

Gebruik een veilig kanaal
Persoonsgegevens deel je niet zomaar via gewone e-mail, gedeelde mappen of informele transferdiensten. Gebruik alleen kanalen en omgevingen die door je organisatie zijn goedgekeurd en voldoende beveiligd zijn. Maak ook afspraken over toegang. Wie mag de data zien? Voor hoe lang? Mag de data gedownload worden? Wordt toegang gelogd? En wie trekt de toegang opnieuw in wanneer de samenwerking stopt?

Denk ook aan het einde van de samenwerking
Maak vooraf afspraken over wat er na afloop gebeurt. Wordt de data verwijderd, terugbezorgd of bewaard? Wie bevestigt dat de data verwijderd is? Hoe lang mogen resultaten of afgeleide bestanden bewaard worden? En wat gebeurt er als er iets misloopt, bijvoorbeeld bij een datalek of verkeerd gebruik?

Checklist
Doel en data

- ❑ We weten waarom data gedeeld of extern verwerkt zou worden.
- ❑ We weten welke data daarvoor echt nodig is.
- ❑ We hebben nagegaan of minder data volstaat.
- ❑ We hebben nagegaan of de data eerst geanonimiseerd of gepseudonimiseerd kan worden.

Partijen en rollen

- ❑ We weten met welke externe partner(s) we willen samenwerken.
- ❑ We weten welke rol elke partner heeft: verwerker, verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke of onderzoekspartner.
- ❑ We hebben de rolverdeling laten nakijken door onze DPO, jurist of privacyverantwoordelijke.

Juridische afspraken

- ❑ We weten of de verwerking in het verwerkingsregister staat of toegevoegd moet worden.
- ❑ We weten welke overeenkomst nodig is, zoals een verwerkersovereenkomst, samenwerkingsovereenkomst of data transfer agreement.
- ❑ We hebben afspraken over het doel van de verwerking, toegelaten gebruik, toegang, beveiliging, bewaartermijn en verwijdering.
- ❑ We weten of de externe partner subverwerkers of andere derde partijen mag inschakelen.

Veilige overdracht en toegang

- ❑ We weten via welk veilig kanaal of platform data gedeeld mag worden.
- ❑ We delen geen gevoelige of persoonsgegevens via gewone e-mail, gedeelde mappen of informele transferdiensten zonder expliciete goedkeuring en passende beveiliging.
- ❑ We weten wie toegang krijgt tot de data.

- ❑ We hebben afspraken over logging, downloadrechten en het intrekken van toegang.

Na afloop en incidenten

- ❑ We hebben afspraken over wat er na afloop met de data gebeurt.
- ❑ We weten wie bevestigt dat data verwijderd, terugbezorgd of veilig bewaard werd.
- ❑ We weten wat er moet gebeuren als er iets misloopt, bijvoorbeeld bij een datalek, foutieve toegang of verkeerd gebruik.

DPO-check

- ❑ We betrekken onze DPO, jurist of privacyverantwoordelijke vóór data gedeeld wordt of een externe partner toegang krijgt.
- ❑ We gaan niet verder met delen, exporteren of extern laten verwerken van persoonsgegevens zolang niet duidelijk is welke afspraken en beveiliging nodig zijn.

Eerste stap

Maak vóór je data deelt een kort datadeel-plan. Noteer minstens:

1. Welke data willen we delen of extern laten verwerken?
2. Waarom is dat nodig?
3. Met welke partner willen we samenwerken?
4. Welke rol heeft die partner?
5. Welke overeenkomst is nodig?
6. Via welk kanaal of platform wordt de data gedeeld?
7. Wie krijgt toegang?
8. Wat gebeurt er met de data na afloop?
9. Wie moet dit goedkeuren vóór we starten?

Leg dit plan voor aan je DPO, jurist of privacyverantwoordelijke voordat je data exporteert, deelt of toegang geeft.

Woordenlijst

- ✓ **Persoonsgegevens:** Alle informatie waarmee je een specifieke persoon kan identificeren. Niet alleen naam en adres, maar ook een nickname gecombineerd met een leeftijd en een stad, een IP-adres, of een verhaal met genoeg specifieke details (dus ook een chatgesprek).
- ✓ **Bijzondere categorieën van persoonsgegevens:** Een speciale groep van gevoelige gegevens waarvoor de GDPR extra strenge regels oplegt. Denk aan gegevens over gezondheid, psychisch welzijn, seksuele geaardheid of etnische afkomst.
- ✓ **Verwerkingsverantwoordelijke:** De organisatie die beslist waarom en hoe persoonsgegevens worden verzameld en gebruikt.
- ✓ **Verwerker:** Een externe partij die in opdracht van jouw organisatie persoonsgegevens verwerkt, maar zelf niet beslist wat ermee gebeurt.
- ✓ **DPO:** De data protection officer of privacyverantwoordelijke. Iemand intern of extern die erop toeziet dat jouw organisatie de GDPR correct naleeft.
- ✓ **Data steward:** De data steward bewaart het dagelijkse overzicht over de data binnen de organisatie: wat staat waar, wie heeft toegang, hoe wordt het gebruikt.
- ✓ **Verwerkingsregister:** Een intern document waarin bijgehouden wordt welke persoonsgegevens verwerkt worden, waarom, hoe lang, en wie er toegang toe heeft. Wettelijk zowat verplicht!

- ✓ **Rechtsgrond:** De wettelijke reden waarom je persoonsgegevens mag verwerken. Zonder rechtsgrond mag je niets doen met persoonsgegevens. Voor organisaties in welzijn en zorg zijn de meest relevante toestemming (consent), algemeen belang, en wetenschappelijk onderzoek.
- ✓ **Consent / Toestemming:** De expliciete, vrijwillige en geïnformeerde toestemming van een persoon om zijn gegevens te gebruiken. Toestemming voor het voeren van een gesprek is niet automatisch toestemming voor het gebruik van dat gesprek in een onderzoeksproject.
- ✓ **Consentformulier:** Het document of de tekst waarmee een gebruiker toestemming geeft voor het gebruik van zijn gegevens. Als je data wil gebruiken voor onderzoek of wil delen met een externe partner, moet dat expliciet in het consentformulier staan.
- ✓ **Anonimisering:** Het proces waarbij persoonsgegevens zo worden aangepast dat het onmogelijk wordt om nog te achterhalen over wie het gaat, ook niet met extra informatie erbij.
- ✓ **Pseudonimisering:** Het proces waarbij persoonsgegevens zo worden aangepast dat zoveel mogelijk herkenbare elementen worden vervangen of weggelaten, maar de data blijft in theorie herleidbaar of reconstrueerbaar als je genoeg context hebt. Pseudonieme data valt nog steeds onder de GDPR.
- ✓ **Verwerkersovereenkomst (DPA):** Een contract tussen jouw organisatie en een externe partij die in jouw opdracht data verwerkt, bijvoorbeeld het bedrijf dat een chat- of e-mailplatform beheert of een AI-tool bouwt.
- ✓ **Data Transfer Agreement (DTA):** Een contract specifiek voor het overdragen van data van de ene organisatie naar de andere, bijvoorbeeld naar een onderzoeksinstelling. Dit kan ook binnen een bredere samenwerkingsovereenkomst. Het legt vast wie wat doet, met welk doel, en onder welke voorwaarden.