

# Data Protection Impact Assessment: Attendi App

Versie 1.1 - 02-12-2025

Eerste publicatie: 10 oktober 2025

Naam: Annemarie Spanjer

Functie: Compliance Officer

## Versiebeheer

| Versie     | Datum      | Auteur     | Beschrijving wijziging                                                                                                                                                                                                                     |
|------------|------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1.1</b> | 02-12-2025 | A. Spanjer | Bewaartermijnen verduidelijkt (24 uur transcript, samenvatting max. 30 dagen). Toelichting rol Attendi als verwerker aangescherpt. Verwijzing naar clauseule voor modelverbetering verwijderd. Versiebeheerproces en changelog toegevoegd. |
| <b>1.0</b> | 10-10-2025 | A. Spanjer | Eerste versie van de DPIA voor de Attendi App.                                                                                                                                                                                             |

## Inhoudsopgave

|                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------|----|
| Versiebeheer .....                                                                                                           | 2  |
| A. Beschrijving kenmerken gegevensverwerkingen .....                                                                         | 4  |
| 1. Beschrijving en scope .....                                                                                               | 4  |
| 2. Persoonsgegevens .....                                                                                                    | 4  |
| 3. Gegevensverwerkingen .....                                                                                                | 6  |
| 4. Verwerkingsdoeleinden .....                                                                                               | 6  |
| 5. Betrokken partijen .....                                                                                                  | 6  |
| 6. Belangen bij de verwerking Het ondersteunen van tijdige, volledige verslaglegging in het kader van de zorgverlening ..... | 7  |
| Met als bijkomend voordeel: .....                                                                                            | 7  |
| 7. Verwerkingslocaties .....                                                                                                 | 7  |
| 8. Techniek en methode van verwerking .....                                                                                  | 7  |
| 9. Bewaartermijnen .....                                                                                                     | 9  |
| B. Beoordeling rechtmatigheid gegevensverwerkingen .....                                                                     | 11 |
| 10. Rechtsgrond .....                                                                                                        | 11 |
| 11. Doelbinding .....                                                                                                        | 12 |
| 12. Noodzaak en evenredigheid .....                                                                                          | 12 |
| 13. Rechten van de betrokkenen .....                                                                                         | 13 |
| C. Risico's en maatregelen - Attendi App .....                                                                               | 14 |
| 14. Tabel risico's en maatregelen .....                                                                                      | 14 |
| D. Conclusie en vervolgacties .....                                                                                          | 22 |
| 15. Slotparagraaf .....                                                                                                      | 23 |
| 16. Disclaimer .....                                                                                                         | 23 |

## A. Beschrijving kenmerken gegevensverwerkingen

### 1. Beschrijving en scope

De Attendi App ondersteunt zorgprofessionals bij het efficiënt en accuraat vastleggen van rapportages via spraak. De app bevat functies voor spraakgestuurd rapporteren, het opnemen van gesprekken en het automatisch samenvatten via templates (standaard of eigen).

De verwerking vindt plaats op Microsoft Azure (Europa) servers. De functionaliteiten worden geleverd door Attendi Technology B.V., die optreedt als verwerker. De verwerkingsverantwoordelijkheid ligt bij de zorgorganisatie die Attendi inzet.

### 2. Persoonsgegevens

| Categorie betrokkenen | Categorie persoonsgegevens       | Persoonsgegevens                                                          | Type (AVG)                       | Bron /herkomst                         | Bewaartermijn                                                           |
|-----------------------|----------------------------------|---------------------------------------------------------------------------|----------------------------------|----------------------------------------|-------------------------------------------------------------------------|
| <b>Cliënten</b>       | Identificatiegegevens            | Voor- en achternaam, cliëntnummer, ECD-ID                                 | Gewoon / identificatie           | Ingevoerd door zorgprofessional / ECD  | Conform bewaartermijn zorgdossier (20 jaar, Wgbo)                       |
|                       | Contactgegevens (indien genoemd) | Telefoonnummer, adres, e-mail                                             | Gewoon                           | Inspraak / notities                    | Alleen zolang notitie in dossier bewaard blijft                         |
|                       | Gezondheidsgegevens              | Medische toestand, behandeling, medicijngebruik, observaties, triage-info | Bijzonder (art. 9 AVG)           | Audio-opname, transcript, samenvatting | 1 maand                                                                 |
|                       | Audio- en transcriptgegevens     | Stemgeluid, uitspraken tijdens zorggesprek                                | Bijzonder (biometrisch mogelijk) | Opname via Attendi App                 | Audio max. 24 uur, transcript max. 24 uur, samenvatting conform dossier |

| Categorie betrokkenen                       | Categorie persoonsgegevens          | Persoonsgegevens                                        | Type (AVG)                                                             | Bron /herkomst                 | Bewaartermijn                                               |
|---------------------------------------------|-------------------------------------|---------------------------------------------------------|------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------|
|                                             | Metadata opname                     | Tijdstip, duur gesprek, device-ID                       | Gewoon / technisch                                                     | Attendi App backend            | Max. 1–2 jaar (logging/technisch beheer)                    |
|                                             | Toestemmingsgegevens (Consent-logs) | Digitale check                                          | Gewoon (juridisch)                                                     | App (pop-up of opname)         | Gedurende de looptijd van de overeenkomst                   |
| <b>Zorg-professionals (gebruikers)</b>      | Accountgegevens                     | Naam, e-mail, werknemers-ID, rol                        | Gewoon / identificatie                                                 | Attendi (SSO/IdP)              | Zolang account actief is                                    |
|                                             | Werkgerelateerde data               | Functie, afdeling, teamnaam toegangsrechten             | Gewoon / identificatie                                                 | HR, SSO/accountbeheer          | Zolang account actief is                                    |
|                                             | Audio- en transcriptgegevens        | Gesproken tekst professional tijdens opname             | Gewoon (kan bijzondere data bevatten in combinatie met cliëntgegevens) | Attendi App                    | Audio/transcript max. 24 uur, samenvatting maximaal 1 maand |
|                                             | Logging / gebruiksdata              | IP-adres, inlogtijd, acties (start opname, goedkeuring) | Gewoon / technisch                                                     | Attendi App (audit trail)      | 1–2 jaar (afhankelijk van klantafspraken)                   |
| <b>Overige betrokkenen (indirect)</b>       | Incidenteel genoemde derden         | Namen van familieleden, mantelzorgers etc               | Gewoon                                                                 | Audio-opname / transcript      | Audio/transcript max. 24 uur, samenvatting maximaal 1 maand |
| <b>Attendi IT- &amp; supportmedewerkers</b> | Support- & beheersdata              | Incidenteel toegang tot metadata, nooit tot inhoud      | Gewoon                                                                 | Supportcases / beheerssystemen | Alleen zolang supportcase loopt                             |

### 3. Gegevensverwerkingen

- Gesprekken met cliënten of collega's kunnen worden opgenomen via de applicatie.
- De audio-opnames worden geüpload en maximaal 24 uur bewaard.
- Transcriptie vindt plaats met een eigen spraak-naar-tekst model dat gebruikmaakt van sprekersherkenning, zodat sprekers afzonderlijk herkend worden.
- Voor het genereren van samenvattingen wordt een Large Language Model (LLM) ingezet.
- De ingevulde templates worden beveiligd opgeslagen.
- Gebruikers kunnen de resultaten downloaden en opslaan in het Elektronisch Cliënten Dossier (ECD).

### 4. Verwerkingsdoeleinden

De verwerking van persoonsgegevens via de Attendi App vindt plaats ter ondersteuning van de zorgverlening, met als concreet doel het op gestructureerde wijze vastleggen van informatie in het kader van de zorgovereenkomst.

### 5. Betrokken partijen

- De zorgorganisatie treedt op als verwerkingsverantwoordelijke.
- Attendi Technology B.V. vervult de rol van verwerker.
- Microsoft Azure wordt ingezet als subverwerker voor hosting en opslag.

#### **Toegang:**

- Zorgmedewerkers hebben uitsluitend toegang tot hun eigen rapportages.
- Alleen geautoriseerde medewerkers van Attendi beschikken over technische toegang (via RBAC, MFA en VPN), maar zij hebben geen operationele toegang tot cliëntdata.

## 6. Belangen bij de verwerking

Het ondersteunen van tijdige, volledige verslaglegging in het kader van de zorgverlening.

Met als bijkomend voordeel:

- Vermindering van administratieve lasten voor zorgmedewerkers
- Versnelling van verslaglegging
- Verbetering van de kwaliteit en volledigheid van het zorgdossier
- Directe omzetting van mondelinge input in gestructureerde rapportages

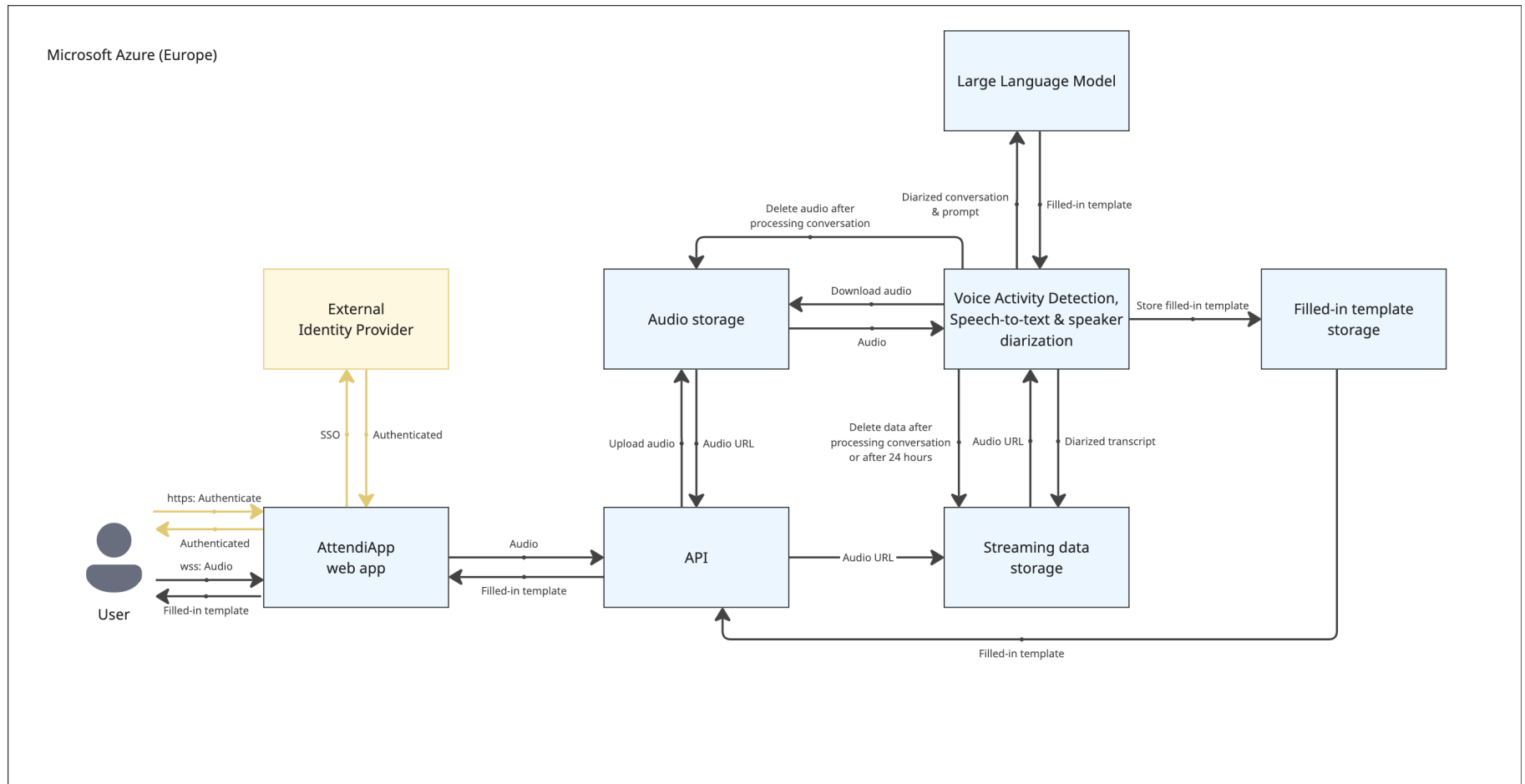
## 7. Verwerkingslocaties

Alle verwerkingen vinden plaats binnen de EER op Microsoft Azure (Europa).

## 8. Techniek en methode van verwerking

| Technische maatregelen |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Invoer:</b>         | Inspreken via native Android/iOS-app of via webapp/plugin.                                                                |
| <b>Transport:</b>      | Alle communicatie verloopt via TLS 1.2+.                                                                                  |
| <b>Opslag:</b>         | Audio, transcript en samenvattingen worden met AES-256 versleuteld; sleutelbeheer via KMS.                                |
| <b>Toegang:</b>        | RBAC, MFA, logging en monitoring. Interne toegang alleen via VPN en Zero Trust.                                           |
| <b>Verwerking:</b>     | Spraak-naar-tekst met sprekersherkenning en LLM voor samenvattingen. Geen geautomatiseerde besluitvorming of profilering. |
| <b>Bewaartermijn:</b>  | Audio en transcript max. 24 uur, samenvattingen blijven maximaal 1 maand bewaard.                                         |

## Methode van verwerking:



## 9. Bewaartermijnen

| Gegevensverwerking                | Verwerkingsdoeleinde                                    | Categorie persoonsgegevens                                    | Bewaartermijn                                                                                                                                           | Motivatie bewaartermijn                                                                              |
|-----------------------------------|---------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Audio-opnames</b>              | Transcriptie genereren                                  | Gesproken tekst (gezondheidsgegevens, NAW indien genoemd)     | Max. 24 uur (technisch afdwingen)                                                                                                                       | Audio enkel nodig voor transcriptie; verwijderen na 24u voorkomt onnodige opslag van gevoelige data. |
| <b>Transcripties (ruwe tekst)</b> | Input voor samenvatting / notitie                       | Gezondheidsgegevens, NAW indien genoemd                       | Max. 24 uur. Na 24 uur wordt de data automatisch verwijderd van alle servers en niet opgenomen in de backups                                            | Transcript alleen nodig voor genereren van samenvatting. Daarna verwijderen minimaliseert risico's.  |
| <b>Samenvattingen / notities</b>  | Dossiervoering / overdracht aan ECD of template storage | Gezondheidsgegevens, cliëntgegevens                           | Samenvattingen worden maximaal 1 maand bewaard. Zowel de cliënt als de zorgprofessional heeft het recht de samenvatting op ieder moment te verwijderen. | Nodig voor medisch dossier; bewaartermijnen volgen uit wetgeving (bijv. 20 jaar medisch dossier).    |
| <b>Metadata (sprekerlabels)</b>   | Verbeteren leesbaarheid transcript / logging            | Technische data, evt. pseudonieme info: spreker 1, spreker 2. | Max. 24 uur. Na 24 uur wordt de data automatisch verwijderd van alle servers en niet opgenomen in de backups                                            | Alleen nodig voor analyse van opname; verwijderen zodra samenvatting definitief is.                  |
| <b>Toestemming (Consent)</b>      | Vastleggen toestemming voor audio-opname                | Gebruikers-ID + datum/tijdstip                                | Consent wordt bewaard gedurende de looptijd van het contract tussen                                                                                     | Aantoonbaar bewijs van toestemming vereist; (voor het aantonen van                                   |

| Gegevensverwerking                  | Verwerkingsdoeleinde                                                                                                                                                                                                                                                 | Categorie persoonsgegevens                                                                                                                                               | Bewaartermijn                                                                                                                  | Motivatie bewaartermijn                                                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                                                                                                                                                                                                                                                      |                                                                                                                                                                          | Attendi en de zorgorganisatie. Zowel de cliënt als de zorgprofessional heeft het recht consent op ieder moment te verwijderen. | naleving AVG art. 5 lid 2). Bewaartermijn in lijn met dossier of behandelovereenkomst.                                                                           |
| <b>Evaluatiedata samenvattingen</b> | Waarborgen van de kwaliteit van verslaglegging door het vergelijken (binnen 24 uur) van transcript en samenvatting, uitsluitend in het belang van de verwerkingsverantwoordelijke (zorginstelling), zodat veelvoorkomen de fouten tijdig kunnen worden gecorrigeerd. | Samenvattingen en bijbehorende transcriptinformatie binnen de eigen omgeving van de zorginstelling; inclusief kwaliteitsindicator (kwaliteitsscore) van de samenvatting. | Uitsluitend gedurende 24 uur voor de kwaliteitscontrole. De evaluatiescore wordt niet verder gebruikt of extern verwerkt.      | Ondersteuning van correcte verslaglegging binnen verantwoordelijkheid van de zorginstelling; geen verwerking voor productontwikkeling of commerciële doeleinden. |

### Toelichting bewaartermijn

Attendi past *privacy by default* toe door verwerkingen zo in te richten dat alleen de minimaal noodzakelijke persoonsgegevens worden gebruikt, bewaard en toegankelijk zijn.

Dit omvat vier concrete maatregelen:

1. **Dataminimalisatie:** alleen gegevens die noodzakelijk zijn voor verslaglegging worden verwerkt; geen additionele metadata of ongebruikte velden.

2. **Beperkte doelbinding:** data wordt uitsluitend verwerkt voor verslaglegging en kwaliteitscontrole binnen 24 uur; er vindt geen verdere verwerking plaats voor productontwikkeling of commerciële doeleinden.
3. **Beperkte bewaartermijnen:** operationele data zoals audio en transcript worden automatisch na 24 uur verwijderd.
4. **Toegangsbeperking:** gegevens zijn alleen toegankelijk voor geautoriseerde zorgprofessionals binnen de tenant van de zorginstelling; Attendi heeft geen toegang tot inhoudelijke cliëntdata.

Consent-gegevens worden technisch gelogd binnen de app. De zorginstelling kan deze informatie desgewenst opvragen voor audit, dossiervorming of klachtenafhandeling.

## B. Beoordeling rechtmatigheid gegevensverwerkingen

### 10. Rechtsgrond

De verwerking van persoonsgegevens in de Attendi App steunt op verschillende grondslagen onder de Algemene verordening gegevensbescherming (AVG), afhankelijk van het type gegevens en de betrokkenen:

- **Zorgcliënten (transcripties en samenvattingen)**  
De verwerking van transcripties en samenvattingen die voortvloeien uit zorggesprekken vindt plaats onder verantwoordelijkheid van de zorgorganisatie en is noodzakelijk voor het uitvoeren van de geneeskundige behandelingsovereenkomst tussen zorgverlener en cliënt (AVG art. 6 lid 1 sub b). Omdat het hier gaat om gezondheidsgegevens, geldt daarnaast de uitzondering van art. 9 lid 2 sub h AVG: de verwerking is noodzakelijk voor het verlenen van gezondheidszorg door een beroepsbeoefenaar die aan het beroepsgeheim is gebonden.
- **Medewerkers (gebruikersaccounts)**  
Voor de verwerking van persoonsgegevens van medewerkers (zoals naam, e-mailadres en gebruikers-ID) geldt als grondslag het gerechtvaardigd belang van de zorgorganisatie (AVG art. 6 lid 1 sub f). Dit belang betreft onder meer toegangsbeheer, autorisatie, beveiliging en logging binnen de applicatie.
- **Audio-opnames van zorggesprekken**  
Het opnemen van gesprekken is een aanvullend hulpmiddel ter ondersteuning van verslaglegging en het genereren van samenvattingen. Omdat de zorgverlening ook zonder opname kan plaatsvinden, is deze verwerking niet strikt noodzakelijk voor de uitvoering van de behandelingsovereenkomst.  
Daarom is voor deze verwerking aparte toestemming vereist:

- **AVG art. 6 lid 1 sub a:** de betrokkene heeft **toestemming** gegeven voor het opnemen van het gesprek.
- **AVG art. 9 lid 2 sub a:** de betrokkene heeft **uitdrukkelijke toestemming** gegeven voor de verwerking van gezondheidsgegevens.

De toestemming ziet dus specifiek op de wijze van gegevensverzameling (audio-opname), niet op de behandeling zelf.

De WGBO vereist dat cliënten vooraf goed worden geïnformeerd en dat toestemming vrijwillig, specifiek en te allen tijde intrekbaar is.

Om aan de verantwoordingsplicht te voldoen (AVG art. 5 lid 2) worden toestemmingen aantoonbaar vastgelegd, doormiddel van registratie van datum, tijdstip en gebruiker in de logbestanden van de applicatie.

De zorgorganisatie is de verwerkingsverantwoordelijke, Attendi B.V. is verwerker. In alle gevallen wordt transparantie geborgd door middel van duidelijke toestemmingsflows, privacyverklaringen, disclaimers in de applicatie en technische controles voor het registreren van de toestemming.

## 11. Doelbinding

De verwerking van persoonsgegevens dient uitsluitend om zorginhoudelijke gesprekken te registreren en te ondersteunen met automatische transcriptie en samenvatting. De gegevens worden niet voor andere doeleinden gebruikt zonder aanvullende toestemming. (conform art. 5 lid 1 sub b AVG). Rapportages worden alleen opgeslagen na controle door de zorgprofessional; dit voorkomt dat art. 22 AVG (geautomatiseerde besluitvorming) in beeld komt.

## 12. Noodzaak en evenredigheid

De verwerking is noodzakelijk om de werkdruk van zorgprofessionals te verlagen en de nauwkeurigheid van rapportages te verhogen. De toepassing is proportioneel, aangezien de gebruiker altijd zelf controle houdt over de inhoud, bewerking en opslag. De technologie wordt alleen toegepast als alternatief voor handmatige verslaglegging.

### 13. Rechten van de betrokkenen

Attendi heeft geen direct contact met de cliënt. Het contact verloopt via de zorginstelling. Om die reden zal de cliënt wanneer hij/zij gebruik wil maken van zijn/haar privacy rechten, in eerste instantie contact opnemen met de zorginstelling.

Op grond van de AVG hebben betrokkenen de volgende rechten ten aanzien van hun persoonsgegevens:

- het recht op inzage;
- het recht op correctie van hun onjuiste gegevens;
- het recht om (verouderde) persoonsgegevens te laten verwijderen;
- het recht om toestemming in te trekken;
- het recht om de verwerking van hun gegevens te laten beperken;
- het recht om hun persoonsgegevens in digitaal leesbaar standaardformaat te verkrijgen en om deze over te (laten) dragen;
- het recht om bezwaar te maken tegen een bepaald gebruik;
- het recht op een menselijke blik bij geautomatiseerde besluitvorming (waaronder profilering);
- het recht om een klacht in te dienen bij een toezichthouder (voor Nederland: de Autoriteit Persoonsgegevens).

Attendi ondersteunt deze rechten technisch via veilige opslag, logging en duidelijke instructies over dataportabiliteit en bezwaarprocedures.

## C. Risico's en maatregelen - Attendi App

### 14. Tabel risico's en maatregelen

Onderstaande tabel geeft een overzicht van de geïdentificeerde risico's bij het gebruik van de Attendi App en de bijbehorende beheersmaatregelen. De maatregelen zijn verdeeld in acties van Attendi (verwerker) en **mogelijke aanvullingen voor de zorginstelling (verwerkingsverantwoordelijke)**.

| Risico                                                                                                                                                           | Oorzaak                                                                                                                            | Waarschijnlijkheid | Impact                                                                                                    | Maatregelen Attendi                                                                                                                                                                                                                                                                        | Voorgestelde maatregelen Zorginstelling                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Onjuiste of onvolledige transcripties                                                                                                                            | Technologische beperkingen: AI-model maakt fouten in spraakherkenning of sprekersherkenning (onderscheiden van 2 of meer personen) | Middelmatig        | Hoog: kan leiden tot verkeerde medische beslissingen                                                      | <ul style="list-style-type: none"> <li>• AI-model getraind op medische context</li> <li>• Continue optimalisatie via feedback</li> </ul>                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Instructie &amp; training in duidelijk spreken</li> <li>• Controle door zorgprofessional verplicht stellen</li> <li>• Bewustwording creëren over risico's</li> </ul>                                                                                   |
| Wanneer de applicatie niet goed functioneert of onverwacht uitvalt, kan de opname of samenvatting mislukken. Dit kan leiden tot verlies van data en het verloren | Technische storing (bv. netwerk, app-crash, fout in verwerking)                                                                    | Middelmatig        | Hoog: verlies van cruciale zorginformatie, risico op gaten in het dossier, verminderde kwaliteit van zorg | <ul style="list-style-type: none"> <li>• Stabiele infrastructuur en monitoring (uptime, foutdetectie)</li> <li>• Heldere foutmeldingen</li> <li>• Logging van falende opnames voor analyse en verbetering (enkel technische aspecten geen inhoud van opnames of samenvattingen)</li> </ul> | <ul style="list-style-type: none"> <li>• Instructie aan zorgprofessionals om bij storingen kernpunten handmatig vast te leggen (pen/papier of ECD)</li> <li>• Bewustwording: AI-app is een hulpmiddel, geen vervanging van professioneel noteren</li> <li>• Procedure bij technische</li> </ul> |

| Risico                                                                                                | Oorzaak                                                                                                      | Waarschijnlijkheid | Impact                                                                                            | Maatregelen Attendi                                                                                                                                                                                                                            | Voorgestelde maatregelen Zorginstelling                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaan van kennis uit het gesprek                                                                       |                                                                                                              |                    |                                                                                                   |                                                                                                                                                                                                                                                | storing (wat te doen als opname mislukt) --> handmatig noteren                                                                                                                                                                         |
| Onbedoelde opname van extra informatie                                                                | Opname blijft per ongeluk aanstaan: menselijke fout                                                          | Middelmatig        | Hoog: onbedoelde gegevens kunnen in dossier terechtkomen                                          | <ul style="list-style-type: none"> <li>• Duidelijke UI/UX voor opnamebeëindiging</li> <li>• Beperkte bewaartermijn van ruwe audio</li> <li>• Logging en audit trails</li> </ul>                                                                | <ul style="list-style-type: none"> <li>• Instructie: actief beëindigen opname</li> <li>• Bewustwording bij medewerkers</li> <li>• Heldere procedure 'wat te doen bij foutopname'</li> </ul>                                            |
| Vertrouwelijkheid van medische gegevens wordt doorbroken (meer data vastgelegd dan zonder AI-systeem) | AI-opname legt meer informatie vast dan traditioneel rapporteren, inclusief irrelevante of gevoelige details | Middelmatig        | Hoog: risico op doorbreken beroepsgeheim, verlies vertrouwen cliënt, meer gevoelige data verwerkt | <ul style="list-style-type: none"> <li>• Alleen noodzakelijke data verwerken (dataminimalisatie in model/app)</li> <li>• UX: duidelijke opnameknop en mogelijkheid pauzeren/hervatten</li> <li>• Tijdelijke opslag (audio max. 24u)</li> </ul> | <ul style="list-style-type: none"> <li>• Cliënt vooraf informeren en toestemming vragen</li> <li>• Procedure: opname starten na koetjes-en-kalfjes-gedeelte</li> <li>• Mogelijkheid bieden aan cliënt om opname te weigeren</li> </ul> |
| Onjuiste correcties door zorgprofessional                                                             | Gebrek aan aandacht of kennis / tijdsdruk                                                                    | Middelmatig        | Hoog: foutieve verslaglegging ondanks transcriptie                                                | <ul style="list-style-type: none"> <li>• Handmatige correctiemogelijkheid</li> <li>• Bewustwording via scholing en instructie</li> </ul>                                                                                                       | <ul style="list-style-type: none"> <li>• Kwaliteitscontrole op rapportages</li> <li>• Periodieke audits of steekproeven</li> </ul>                                                                                                     |

| Risico                                                     | Oorzaak                                                                                | Waarschijnlijkheid                           | Impact                                                           | Maatregelen Attendi                                                                                                                                                                                                                        | Voorgestelde maatregelen Zorginstelling                                                                                                                                                                                                                              |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inspreken van irrelevante of foutieve info                 | Gebrek aan concentratie: context verkeerd ingeschat                                    | Laag                                         | Middelmatig: extra verwerkingstijd of verkeerde interpretatie    | <ul style="list-style-type: none"> <li>• Trainingsmodule over gebruik</li> <li>• AI probeert irrelevante info te filteren</li> </ul>                                                                                                       | <ul style="list-style-type: none"> <li>• Interne richtlijnen voor dicteren</li> <li>• Awareness vergroten via onboarding</li> <li>• Mogelijkheid tot niet overnemen/ verwijderen transcript of samenvatting</li> </ul>                                               |
| Onvoldoende controle voor opslaan rapportage               | Menselijke fout: onvoldoende nadruk op nacontrole                                      | Middelmatig                                  | Hoog: onjuiste info wordt definitief opgeslagen                  | <ul style="list-style-type: none"> <li>• Opslag pas na expliciete goedkeuring</li> <li>• Instructie in app en onboarding</li> </ul>                                                                                                        | <ul style="list-style-type: none"> <li>• Procedure verplicht nalezen voor opslaan</li> <li>• Logging op wie wanneer opslaat</li> </ul>                                                                                                                               |
| Ongeautoriseerde toegang tot samenvattingen in database    | Attendi developers hebben in theorie toegang tot opgeslagen notities                   | Laag                                         | Hoog: privacyrisico bij toegang tot medische gegevens            | <ul style="list-style-type: none"> <li>• Toegang beperkt tot bevoegde developers</li> <li>• ISO 27001 en NEN 7510 maatregelen voor toegangsbeheer</li> </ul>                                                                               | <ul style="list-style-type: none"> <li>• Verwerkersovereenkomst met toegangsafspraken</li> <li>• Vraag om toegangsinzage in audits</li> </ul>                                                                                                                        |
| Onrechtmatige toegang tot cliëntgegevens (intern / extern) | Onvoldoende toegangsbeheer, misbruik van accounts, phishing, technische kwetsbaarheden | Laag (Attendi), Middelmatig (zorginstelling) | Hoog: inbreuk op vertrouwelijkheid van medische persoonsgegevens | <ul style="list-style-type: none"> <li>• Toegang tot cliëntdata is niet mogelijk voor Attendi-medewerkers.</li> <li>• Strikte toegangscontrole en autorisatie op infrastructuur (Azure).</li> <li>• MFA en encryptie toegepast.</li> </ul> | <ul style="list-style-type: none"> <li>• Sterk toegangsbeheer en rolafspraken.</li> <li>• MFA / SSO voor gebruikersaccounts.</li> <li>• Logging en controle van gebruikersactiviteiten.</li> <li>• Regelmatige bewustwordingstrainingen en phishingtests.</li> </ul> |

| Risico                                        | Oorzaak                                                                  | Waarschijnlijkheid                           | Impact                                                             | Maatregelen Attendi                                                                                                                                                                                                                                                                                           | Voorgestelde maatregelen Zorginstelling                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ongewenste wijziging van gegevens             | Menselijke fout, misbruik door onbevoegde gebruiker, malware of hacking. | Laag (Attendi), Middelmatig (zorginstelling) | Hoog: incorrecte of gemanipuleerde medische informatie in dossiers | <ul style="list-style-type: none"> <li>• Attendi-medewerkers kunnen geen cliëntdata wijzigen.</li> <li>• Gebruik van versiebeheer en back-ups.</li> <li>• ISO27001/ NEN7510-processen voor beveiliging en logging.</li> </ul>                                                                                 | <ul style="list-style-type: none"> <li>• Procedure voor dubbele controle van belangrijke wijzigingen.</li> <li>• Logging en monitoring van wie wat wijzigt.</li> <li>• Training medewerkers over juiste verwerking en verslaglegging.</li> <li>• Incidentproces voor herstel en correctie van fouten.</li> </ul>                                                              |
| Audio of transcripten blijven te lang bewaard | Technische fout of gebrekkige bewaarbeleidinstellingen                   | Laag                                         | Hoog: onnodige opslag van gevoelige data                           | <ul style="list-style-type: none"> <li>• Automatische verwijdering na 24 uur ingesteld</li> <li>• Logging van bewaartermijnen</li> <li>• Regelmatige review van opslagconfiguratie</li> </ul>                                                                                                                 | <ul style="list-style-type: none"> <li>• Controleer of verwerkerscontract bewaartermijnen afdekt</li> </ul>                                                                                                                                                                                                                                                                   |
| Geen bewijs van toestemming cliënt            | Toestemming wordt niet opgeslagen of aantoonbaar vastgelegd              | Middelmatig                                  | Hoog: niet kunnen aantonen van AVG-conforme verwerking             | <ul style="list-style-type: none"> <li>• App vraagt expliciet om toestemming vóór de opname (zonder akkoord start de opname niet).</li> <li>• Toestemming wordt automatisch gelogd met datum, tijdstip en gebruikers-ID. (minimale metadata)</li> <li>• Deze logging is beschikbaar te stellen aan</li> </ul> | <ul style="list-style-type: none"> <li>• Leg in de behandelovereenkomst vast dat medische gegevens verwerkt worden voor verslaglegging en dossiervoering (juridische basis).</li> <li>• Zorginstelling borgt dat toestemming voor opname altijd expliciet en per situatie wordt gevraagd (WGBO) en legt dit vast in duidelijke richtlijnen voor zorgprofessionals.</li> </ul> |

| Risico                                                                              | Oorzaak                                                                           | Waarschijnlijkheid | Impact                                                                                   | Maatregelen Attendi                                                                                                                                                                                                                                                                                                       | Voorgestelde maatregelen Zorginstelling                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                     |                                                                                   |                    |                                                                                          | de zorginstelling als bewijs voor interne audits en compliance<br><ul style="list-style-type: none"> <li>• Logging wordt beveiligd opgeslagen en valt onder de bewaartermijnen en toegangsbeperkingen van Attendi.</li> </ul>                                                                                             | <ul style="list-style-type: none"> <li>• Gebruik de consent-logging als onderdeel van aantoonbaarheid (art. 5 lid 2 AVG verantwoordingsplicht) tbv audits of klachtenbehandeling.</li> <li>• Toestemmingsregistratie zo nodig integreren in cliëntdossier.</li> </ul> |
| Cliënt of hulpverlener spreekt zich niet volledig uit door opname (chilling effect) | Onbehagen bij opname leidt tot weglaten van cruciale informatie                   | Middelmatig        | Hoog: onvolledig dossier, gemiste signalen in zorgverlening                              | <ul style="list-style-type: none"> <li>• Training zorgprofessionals: benoemen van <i>chilling effect</i> en actief navragen</li> </ul>                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• Protocol: bespreekbaar maken van opname bij start gesprek</li> <li>• Scholing medewerkers: herkennen en mitigeren van dit risico</li> </ul>                                                                                  |
| Overreliance op AI-output                                                           | Gebruiker neemt AI-output automatisch over zonder eigen professionele beoordeling | Middelmatig        | Hoog: foutieve of ongecontroleerde informatie in dossier, verlies van menselijke control | <ul style="list-style-type: none"> <li>• AI-disclaimer zichtbaar bij gegenereerde output ("Deze tekst is automatisch gegenereerd met behulp van AI. Controleer altijd op juistheid voor gebruik.")</li> <li>• Gebruiker moet output expliciet bevestigen voor opslag</li> <li>• Instructie over beperkingen AI</li> </ul> | <ul style="list-style-type: none"> <li>• Zorgprofessional verplicht laten controleren en accorderen</li> <li>• Scholing over risico's van overreliance</li> <li>• Interne richtlijn of checklist voor beoordelen AI-output</li> </ul>                                 |
| Onvoldoende logging van AI-beslissingen: AI-samenvattingen zijn                     | Gebrek aan technische inrichting of vergeten bij het ontwerp                      | Laag               | Hoog: beperkt recht op inzage/correctie                                                  | <ul style="list-style-type: none"> <li>• Logging van versie en modeloutput</li> </ul>                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• Interne afspraken over bewaren originele input</li> </ul>                                                                                                                                                                    |

| Risico                                                                                                                            | Oorzaak                                                          | Waarschijnlijkheid | Impact                                                                                                                       | Maatregelen Attendi                                                                                                                                 | Voorgestelde maatregelen Zorginstelling                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| niet traceerbaar naar bronmateriaal                                                                                               |                                                                  |                    | en maakt transparantie en verantwoording moeilijk (AVG art. 5, AI Act)                                                       |                                                                                                                                                     |                                                                                                                                                                                    |
| Gebrek aan uitleg ('explainability') bij AI-samenvatting<br>Gebruiker begrijpt niet waarom bepaalde info wel/niet is opgenomen    | AI-model is een blackbox of gebruikt impliciete selectiecriteria | Middelmatig        | Middelmatig: gebruiker begrijpt niet waarom bepaalde info wel/niet is opgenomen → risico op verkeerd gebruik of overreliance | <ul style="list-style-type: none"> <li>• AI-disclaimer zichtbaar</li> </ul>                                                                         | <ul style="list-style-type: none"> <li>• Training over AI-gedrag en beperkingen</li> <li>• Feedbackloop inbouwen zodat zorgprofessionals onduidelijkheden kunnen melden</li> </ul> |
| Foutieve tagging of templating van rapportages<br>AI voegt verkeerde structuur of labels toe (bv. 'probleem' i.p.v. 'observatie') | AI-model maakt verkeerde inschatting van inhoud/context          | Laag               | Middelmatig: verkeerde interpretatie in dossier kan rechten van cliënt raken (juistheid, art. 5 AVG)                         | <ul style="list-style-type: none"> <li>• Validering door gebruiker voor opslaan</li> <li>• Templates vooraf getest met zorgprofessionals</li> </ul> | <ul style="list-style-type: none"> <li>• Interne richtlijnen bij gebruik templates</li> </ul>                                                                                      |

| Risico                                                             | Oorzaak                                                                | Waarschijnlijkheid | Impact                                                                           | Maatregelen Attendi                                                                                                                                                                                                          | Voorgestelde maatregelen Zorginstelling                                                                                                                                                           |
|--------------------------------------------------------------------|------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rapportage is onjuist/onvolledig door AI-hallucinaties of bias     | Modelfouten, onjuiste interpretatie, beperkte dataset, bias in taal    | Middelmatig        | Hoog: verkeerde zorgbeslissingen of discriminatie                                | <ul style="list-style-type: none"> <li>• Continue training model op medische context</li> <li>• Validatie via feedbackloop en steekproeven</li> <li>• AI-Disclaimer in app en verplicht accorderen door gebruiker</li> </ul> | <ul style="list-style-type: none"> <li>• Controle door zorgprofessional verplicht</li> <li>• Audit op rapportages (steekproeven)</li> <li>• Richtlijn: AI-output nooit blind overnemen</li> </ul> |
| Rapportage terecht bij verkeerde cliënt (mislinking)               | Menselijke fout (kopiëren/plakken), fout in koppeling of identificatie | Laag/Middelmatig   | Hoog: onjuiste gegevens gekoppeld, schending AVG                                 | <ul style="list-style-type: none"> <li>• Technische koppeling naar ECD via zorgprofessional-ID en unieke cliënt-ID's</li> </ul>                                                                                              | <ul style="list-style-type: none"> <li>• Controleprocedure: interne steekproeven en dubbele check</li> <li>• Bewustwordingstraining medewerkers</li> </ul>                                        |
| Non-verbale communicatie ontbreekt in verslag                      | AI legt alleen gesproken tekst vast, geen lichaamstaal of context      | Middelmatig        | Middelmatig: risico op verlies nuance, onvolledig dossier                        | <ul style="list-style-type: none"> <li>• Mogelijkheid notitie toevoegen naast AI-samenvatting</li> </ul>                                                                                                                     | <ul style="list-style-type: none"> <li>• Scholing: zorgprofessional voegt zelf non-verbale observaties toe</li> <li>• Interne richtlijn: direct aanvullen in verslag</li> </ul>                   |
| Gebruik van AI door stagiairs/onervaren gebruikers zonder controle | Onvoldoende toegangsbeheer of rollenstructuur                          | Middelmatig        | Middelmatig: verhoogde kans op fouten, impact op zorgkwaliteit en privacy cliënt | <ul style="list-style-type: none"> <li>• Aparte rechtenstructuur/toegang AI-tools</li> <li>• Logging per rol of gebruiker</li> </ul>                                                                                         | <ul style="list-style-type: none"> <li>• Toezicht op gebruik door leidinggevende</li> <li>• Verplicht meelezen of dubbelcheck</li> </ul>                                                          |

| Risico                                                                         | Oorzaak                                                                  | Waarschijnlijkheid | Impact                                                                                          | Maatregelen Attendi                                                                                                                                      | Voorgestelde maatregelen Zorginstelling                                                                                                                                              |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Foutdetectie faalt door contextverschil (bv. dialect, emoties, ironie)         | Taalmodel herkent geen taalvariaties                                     | Middelmatig        | Laag/<br>Middelmatig:<br>risico op foutieve verslaglegging, raakt juistheid en begrijpelijkheid | <ul style="list-style-type: none"> <li>• Doorlopend verbeteren model met feedback</li> <li>• Niet blind corrigeren op taalniveau</li> </ul>              | <ul style="list-style-type: none"> <li>• Bewustwording over deze zwakke punten</li> <li>• Optie tot handmatige override</li> </ul>                                                   |
| Gebruik van AI-output voor secundaire doeleinden (zoals training of marketing) | Onvoldoende juridische of organisatorische scheiding tussen verwerkingen | Laag               | Hoog: schending doelbinding (AVG art. 5) en risico op misbruik van medische data                | <ul style="list-style-type: none"> <li>• Duidelijke scheiding tussen live data en trainingsdata</li> <li>• Geen hergebruik zonder toestemming</li> </ul> | <ul style="list-style-type: none"> <li>• Vragen bij contractafspraken</li> <li>• Privacybeleid controleren</li> </ul>                                                                |
| Apparaat van zorgprofessional onvoldoende beveiligd (lek via device)           | Gebruik van privételefoon of slecht beveiligde apparatuur                | Laag               | Hoog: opname kan uitlekken via onbeveiligd device                                               | <ul style="list-style-type: none"> <li>• Encryptie van data-at-rest en in-transit</li> </ul>                                                             | <ul style="list-style-type: none"> <li>• Device management en securitybeleid (MFA, encryptie, patching)</li> <li>• Intern protocol: gebruik alleen goedgekeurde apparaten</li> </ul> |

**Laag** = onwaarschijnlijk / uitzonderlijk

**Middelmatig** = mogelijk onder normale omstandigheden

**Hoog** = waarschijnlijk / regelmatig

## D. Conclusie en vervolgacties

De uitvoering van deze DPIA laat zien dat de verwerking van persoonsgegevens binnen de Attendi App in de kern gerechtvaardigd en uitvoerbaar is, mits de genoemde en voorgestelde maatregelen worden getroffen en geborgd. De belangrijkste risico's hebben betrekking op transparantie richting cliënten, het borgen van toestemming voor audio-opnames en het voorkomen van onjuiste of onvolledige rapportages. Voor deze risico's zijn mitigerende maatregelen benoemd die zowel door Attendi als door de zorginstelling geïmplementeerd moeten worden.

De zorgorganisatie dient te beoordelen of de door Attendi beschreven technische en organisatorische maatregelen aansluiten bij de normen van ISO 27001 en NEN 7510. Attendi beschikt over een geldig ISO 27001 en NEN 7510 certificaat en onderhoudt een actief ISMS, inclusief verbeterregister en periodieke evaluatie van maatregelen. Het uitblijven van controles door de zorginstelling ontslaat Attendi niet van de verplichting om deze maatregelen structureel te onderhouden.

De zorginstelling blijft als verwerkingsverantwoordelijke verantwoordelijk voor toezicht op de juiste toepassing van maatregelen in de praktijk. Dit omvat tevens een periodieke toetsing (PDCA-aanpak) van de belangrijkste beheersmaatregelen, zoals:

- toegangs- en autorisatiebeheer
- logging en monitoring
- bewaartermijnen
- correcte vastlegging en verificatie van toestemmingen
- naleving van procedures rondom incidentmeldingen en beveiligingscontroles

Attendi voldoet als verwerker aan alle relevante verplichtingen uit de AVG en de UAVG en borgt deze binnen het eigen ISMS.

## 15. Slotparagraaf

Dit DPIA-document is opgesteld als hulpmiddel om risico's vroegtijdig te identificeren en te beheersen. Het is geen statisch document, maar een levend instrument: bij wijzigingen in processen, technologie, productfunctionaliteit of wetgeving moet de DPIA opnieuw worden beoordeeld en geactualiseerd. Door dit periodiek te doen, blijven zowel de juridische als praktische waarborgen actueel en effectief.

## 16. Disclaimer

Deze DPIA is opgesteld op basis van de informatie die op **2 december 2025** beschikbaar was. De beoordeling en voorgestelde mitigerende maatregelen zijn onder voorbehoud van toekomstige wijzigingen in processen, technologie of wet- en regelgeving. De verwerkingsverantwoordelijke blijft te allen tijde eindverantwoordelijk voor naleving van de AVG en relevante normen. Bij substantiële wijzigingen in de verwerking dient de Data Protection Impact Assessment opnieuw te worden beoordeeld en geactualiseerd.