Steedsverbeteren
kwaliteitsmanagement | informatiebeveiliging

prospectief

Prospectief BV

Data Protection Impact Assessment (DPIA)

Gebruik AI-tool

Versie:	2
Datum:	13-07-2026
Classificatie:	vertrouwelijk

Inhoudsopgave

INLEIDING, MANAGEMENTSAMENVATTING EN CONCLUSIE 4

1. Inleiding 4
A. Algemeen 4
B. Geraadpleegde documentatie 4
C. DPIA en verantwoording gebruikte methodiek 5
D. Uitvoering van de DPIA 5
E. Betrokkenheid Functionaris Gegevensbescherming 5
F. Leeswijzer 5

2. Managementsamenvatting en conclusie 6
G. Aanbevelingen 8

RAPPORTAGE UITGEVOERDE DPIA 12

3. Systematische beschrijving van de verwerkingen en de verwerkingsdoelen 13
H. Inventarisatie 13
I. Analyse hoog privacyrisico 14

4. AI-systemen en de risico's 20
J. Systemen met een onaanvaardbaar risico: verboden AI 20
K. Systemen met een hoog risico 21
L. Systemen met een beperkt risico 22
M. Systemen met een laag risico 22
N. Systemen aan te merken als medisch hulpmiddel 22

5. Algoritmen of model (eventueel aanbieder betrekken bij dit hoofdstuk) 23
O. Doel 23
P. Werking 23
Q. Data 24
R. Biases 25
S. Transparantie 25
T. Gevolgen gebruik algoritme 26
U. Nauwkeurigheid en betrouwbaarheid 27
V. Privacy en veiligheid van gegevens 27
W. Aanpassen of stoppen indien nodig 29
X. Gebruikers 29

Y. Verantwoordelijkheid 30
Z. Vereisten voor systemen met een hoog risico 31
AA. Vereisten voor systemen met een beperkt risico 33

6. Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking 35

7. Risicobeoordeling voor betrokkenen 36

8. Is voorafgaande raadpleging AP nodig? 38

9. Monitoring en evaluatie 38

10. Ondertekening 38

BIJLAGEN 39

Bijlage 1 Privacy principes 39

Bijlage 2 Grondslagen 41

Bijlage 3 Doelbinding 43

Bijlage 4 Rechten van betrokkene 44

Bijlage 5 Algoritme 45

Bijlage 6 Algoritmeregister van de Nederlandse overheid 46

Bijlage 7 Bias 48

Bijlage 8 Definities 50

INLEIDING, MANAGEMENTSAMENVATTING EN CONCLUSIE

1. Inleiding

A. Algemeen

Prospectief BV heeft Steeds Verbeteren BV gevraagd een Data Protection Impact Assessment (DPIA) uit te voeren op het gebruik van een AI-tool bij het:

- Samenvatting van medische dossiers
- Identificatie van relevante medische en juridische argumenten
- Conceptanalyse en rapportage ter ondersteuning van de professional
- Interne kennisondersteuning (bijv. opzoeken van richtlijnen, ICF-classificatie)

De AI-tool helpt de medewerker van Prospectief BV bij het doorwerken van een klantdossier: het maakt een gestructureerde samenvatting en signaleert relevante feiten. Hierdoor kan de medewerker van Prospectief BV de zaak sneller en vollediger beoordelen. De AI-tool neemt geen beslissingen het levert een voorbereiding die de medewerker vervolgens zelfstandig beoordeelt, aanvult en waar nodig corrigeert. De medewerker draagt de volledige professionele verantwoordelijkheid voor het eindresultaat.
De verwerking betreft gepseudonimiseerde gezondheidsgegevens. Deze gegevens blijven persoonsgegevens in de zin van de AVG.

Hierbij treft u de DPIA-rapportage aan. Deze DPIA is uitgevoerd op de verwerkingen van persoonsgegevens van Prospectief BV in haar rol van (toekomstige) Arbodienst en in het proces arbodienstverlening en bezwaar en beroep. De overige verwerkingen van persoonsgegevens binnen en buiten Prospectief BV (denk hierbij aan het verwerken van persoonsgegevens van de eigen medewerkers) zijn buiten de scope.

B. Geraadpleegde documentatie

- (v2 4_3_26) Nebelus - Scope of Certification Statement
- (v3 4_3_26) Nebelus - Statement of Applicability (SOA)
- (v3 6_10_26) Nebelus - Data Processing Agreement
- AI Systeemkaart Nebelus AI Studio
- DPIA_NovaLink-Nebelus_v2.0
- EU-Only Processing Attestation v2
- Informatiebrief
- Intern AI Beleid Prospectief
- NEBELUS_GR25_EIAC-Cert
- Privacyverklaring_voorstel_definitief (1)
- Procedural Summaries - Data Breach, DSAR, and Deletion
- Pseudonimisatieprotocol
- Sample Deletion Confirmation Report)
- Subverwerkersovereenkomst_Novalink_Nebelus
- Verwerkersovereenkomst_Prospectief_Novalink_definitief

C. DPIA en verantwoording gebruikte methodiek

Een kernverplichting uit de Algemene Verordening Gegevensbescherming (AVG) is dat organisaties moeten kunnen aantonen dat hun gegevensverwerkingen voldoen aan de regels uit de AVG. Een belangrijk instrument uit de AVG om dat te doen is het uitvoeren van een zogenaamde Data Protection Impact Assessment (DPIA). Met deze risicoanalyse worden privacyrisico's van een gegevensverwerking in kaart gebracht en is men in staat om passende maatregelen te nemen om de risico's te verkleinen en te beheersen.

De wijze van uitvoering van een DPIA is vormvrij en er zijn verschillende methodes om een DPIA uit te voeren. De gevolgde methodiek is gebaseerd op het model uit het boek Handleiding DPIA's[1] . Dit model is ontwikkeld op basis van diverse DPIA-standaarden (waaronder het Nederlandse DPIA Rijksmodel en de DPIA-modellen van de CNIL (Franse toezichthouder) en de ICO (Engelse toezichthouder). Hiermee wordt geborgd dat de DPIA voldoet aan de eisen van de AVG. De uitgevoerde DPIA omvat daarom een systematische beschrijving van de gegevensverwerking, een beoordeling van de rechtmatigheid, van de privacyrisico's en de maatregelen om de risico's aan te pakken.

D. Uitvoering van de DPIA

Op 15 juni jl. en 13 juli jl. is een werksessie gehouden om de verwerking en daarmee ook de daarbij aanwezige privacyrisico's en benodigde beheersmaatregelen in beeld te brengen. Aan die sessie hebben de volgende personen deelgenomen:

- Prospectief BV, Ulla Al-Saad (Algemeen Directeur)
- Prospectief BV, Shajan Omar (Operationeel manager)
- Steeds Verbeteren BV, Christel Bastiaenssens (externe FG)

De uitkomsten van deze werksessie zijn weergegeven in dit rapport.

E. Betrokkenheid Functionaris Gegevensbescherming

Prospectief BV heeft een functionaris voor de gegevensbescherming (FG) aangesteld. De FG is betrokken geweest bij de uitvoer van de DPIA. Dit geeft extra zekerheid dat de DPIA voldoende zicht biedt op de risico's en dat er voldoende maatregelen worden getroffen om deze af te dekken.

F. Leeswijzer

Na deze inleiding treft u de uitkomsten aan van het rapport. Dit bestaat uit de volgende onderdelen.

- Managementsamenvatting en conclusie (inclusief aanbevelingen)
- Rapportage uitgevoerde DPIA
- Bijlagen

[1] Dit is een boek dat de theorie en de praktijk van een uit te voeren DPIA beschrijft. Auteurs: Mr. F. Joung en Mr. S. van de Molen.

2. Managementsamenvatting en conclusie

Naar aanleiding van de bijgewoonde sessies, de beoordeling van de verstrekte documentatie en de uitgevoerde analyse van de voorgenomen verwerking, zijn geen directe blokkades voor ingebruikname van de AI-tool vastgesteld.

Positief is dat bij de inrichting van deze AI-toepassing tevens een ter zake gespecialiseerde jurist betrokken is geweest. Hierdoor is niet alleen aandacht besteed aan privacy- en informatiebeveiligingsaspecten, maar ook aan de juridische grondslagen, contractuele afspraken en de toepassing van relevante wet- en regelgeving.

Op basis van de beschikbare informatie acht ik de juridische, organisatorische en technische basis voor de voorgenomen verwerking grotendeels aanwezig. De verwerking van gezondheidsgegevens kan rechtmatig plaatsvinden binnen de bestaande wettelijke kaders, mits de beschreven maatregelen worden geïmplementeerd, onderhouden en periodiek worden geëvalueerd.

Daarnaast stel ik vast dat:

- de AI-tool uitsluitend beslissingsondersteunend wordt ingezet;
- de uiteindelijke beoordeling, advisering en besluitvorming altijd plaatsvinden door een menselijke professional;
- geen sprake is van geautomatiseerde besluitvorming in de zin van artikel 22 AVG;
- persoonsgegevens voorafgaand aan verwerking worden gepseudonimiseerd;
- passende technische en organisatorische beveiligingsmaatregelen zijn getroffen;
- betrokkenen worden geïnformeerd over de inzet van AI en hun rechten kunnen uitoefenen.

Classificatie AI Act

Op basis van de uitgevoerde beoordeling concludeer ik dat de AI-toepassing niet kwalificeert als een verboden AI-systeem of als een hoog-risico AI-systeem in de zin van de AI Act. De toepassing betreft een ondersteunend systeem voor dossieranalyse en informatieverwerking waarbij menselijk toezicht is geborgd. Classificatie AI Act: AI-systeem met beperkt risico (Limited Risk AI System).

Risico’s

Naar aanleiding van de gehouden sessies zijn voor betrokkenen geen risico’s in de categorie ‘Hoog’ geconstateerd, 9 risico’s in de categorie ‘Midden’ en 8 risico’s in de categorie ‘Laag’. De risico’s in de categorie ‘midden’, vallen in deze categorie omdat in geval van een incident de impact voor betrokkene (persoonlijke gezondheidsinformatie) hoog kan zijn. Eén risico in de categorie ‘Midden’ is te verlagen naar ‘Laag’ indien daadwerkelijk aangetoond kan worden dat er geen toegang vanuit derde landen plaatsvindt. Deze actie is opgenomen bij de alinea ‘Aanbevelingen’.

Ondanks de getroffen technische, organisatorische en contractuele maatregelen blijven enkele restrisico’s bestaan. De belangrijkste restrisico's betreffen:

- verlies van vertrouwelijkheid van gezondheidsgegevens;
- onjuiste AI-output (hallucinaties of onvolledige analyses);
- automation bias (te veel vertrouwen op AI-output door gebruikers);
- verwerking van gegevens van kwetsbare betrokkenen;

- afhankelijkheid van leveranciers en onderliggende AI-diensten.

Gelet op de getroffen beheersmaatregelen, het verplichte menselijke toezicht, de aanwezige beveiligingsmaatregelen en het ontbreken van geautomatiseerde besluitvorming worden deze restrisico's door de Functionaris Gegevensbescherming beoordeeld als beheersbaar en acceptabel.

De resterende aandachtspunten (zie Aanbevelingen) hebben voornamelijk betrekking op aantoonbaarheid, (AI-) governance, compliance en leveranciersmanagement. Hierbij valt onder meer te denken aan het verder formaliseren van AI-geletterdheid, leveranciersdossiers, logreview, bewaartermijnen, pseudonimisatievalidatie, documentatie van beheerlocaties en de expliciete vastlegging van verantwoordelijkheden rondom AI-beheer.

Beoordeling Functionaris Gegevensbescherming

Op basis van de uitgevoerde DPIA, de beschikbare documentatie en de getroffen maatregelen beoordeelt de Functionaris Gegevensbescherming de voorgenomen verwerking als toelaatbaar. Er zijn geen resterende hoge risico's vastgesteld die ingebruikname van de AI-tool verhinderen of voorafgaande raadpleging van de Autoriteit Persoonsgegevens noodzakelijk maken.

Besluit en acceptatie restrisico's door directie

De directie van Prospectief BV heeft kennisgenomen van:

- de uitgevoerde DPIA;
- de geïdentificeerde risico's;
- de getroffen beheersmaatregelen;
- de resterende restrisico's;
- het advies van de Functionaris Gegevensbescherming.

De directie beoordeelt de resterende restrisico's als acceptabel in relatie tot het beoogde doel, de getroffen maatregelen en de verwachte voordelen van de AI-toepassing voor de dienstverlening. Op basis hiervan stemt de directie in met de ingebruikname van de AI-tool.

G. Aanbevelingen

1. In de privacyverklaring staat: Prospectief is ISO 9001- en NEN 7510-gecertificeerd. Dit is niet juist. Prospectief is niet NEN7510-gecertificeerd. Ik adviseer de huidige (correcte) privacyverklaring aan te vullen met AI, aangezien in de huidige verklaring ook zaken staan die voorgeschreven zijn vanuit het CSA.

2. Daarnaast staat in de privacyverklaring:

Arbodienstverlening	grondslag: Art. 6 lid 1 sub b AVG (overeenkomst) + art. 9 lid 2 sub h AVG (geneeskundige beoordeling)	Beoordeling door een BIG-geregistreerde arts met geheimhoudingsplicht, conform art. 30 lid 3 sub a UAVG

   De privacyverklaring noemt als grondslag voor arbodienstverlening artikel 6 lid 1 sub b AVG en artikel 9 lid 2 sub h AVG. Kunt je bevestigen voor welke processen de AI-tool wordt ingezet?

   Voor arbodienstverlening ligt de grondslag veelal in de uitvoering van wettelijke verplichtingen op grond van de Arbeidsomstandighedenwet en aanverwante regelgeving.

3. In de verwerkersovereenkomst Prospectief – Novalink staat als verwerking: Cliënten van VV in bezwaar- en beroepsprocedures. Wordt de AI-tool niet ingezet voor arbodienstverlening?

4. In de verwerkersovereenkomst Prospectief – Novalink staan Technische en organisatorische maatregelen genoemd. Voeg hieraan toe: bewustwordingssessies, toegang o.b.v. need to know, werken onder geheimhouding.

5. Geen toegang buiten de EER aantonen
   Aantonen waar beheerders zich bevinden en dat geen toegang vanuit derde landen mogelijk is.
   Bijvoorbeeld:

Platformbeheer	land x
Security	land y
Support	land x

   Wellicht toevoeging aan verwerkersovereenkomst: beheer- en supporttoegang tot persoonsgegevens vindt uitsluitend plaats vanuit de Europese Economische Ruimte.

   Toegang buiten EER kan gecheckt worden dmv auditlogs.

6. Bewaartermijnen in kaart brengen voor bronbestanden (bijv. medische dossiers, rapporten enz), chunks, embeddings, auditlogs en back-ups documenteren.
   Als aangegeven wordt dat bestanden verwijderd worden, dan wil je ook graag weten of ook alle bestanden uit de verwerkingsslagen (chunks, embeddings) verwijderd worden.

7. Leveranciersmanagement Nebelus en Novalink
   Leveranciersdossier aanleggen en stukken documenteren, checklist kritische cloud leverancier invullen t.b.v. Nebulus, opnemen op leverancierslijst en leveranciersbeoordeling uitvoeren conform het leveranciersproces).

   Verklaring van Toepasselijkheid Nebelus opvragen: zat niet tussen de stukken!

8. Managementsamenvatting pentest opvragen bij Nebelus (**Inmiddels gereed**).

9. Verwerkingsregister actualiseren
   AI-verwerking, leveranciers en technische verwerkingen (pseudonimisering) en organisatorische/technische maatregelen opnemen.

10. Effectiviteit pseudonimisering
    Vastleggen hoe de effectiviteit van de pseudonimisering wordt beoordeeld en gedocumenteerd. Bijvoorbeeld door middel van een periodieke steekproef waarbij wordt beoordeeld of dossiers zonder aanvullende informatie redelijkerwijs herleidbaar zijn.

    Wie beheert de koppelsleutel en welke functies hebben toegang tot deze sleutel? Graag opnemen in de autorisatiematrix.

11. Exit-strategie
    Vastleggen exitstrategie bij beëindiging (dataretour en vernietiging) met Nebelus.

12. Rechten van betrokkenen
    Verifiëren dat bestaande AVG-processen voor inzage, correctie en verwijdering ook betrekking hebben op de AI-verwerking, inclusief eventuele embeddings, logs en afgeleide gegevens.

13. AI-geletterdheid aantonen
    Trainingen, deelnemers en herhalingen documenteren. Gebruik hiervoor ook de Competentiematrix.

14. Kwaliteitsmetingen AI-output
    Periodiek verifiëren dat de in het AI-beleid beschreven kwaliteitsborging (steekproeven, gebruikersfeedback, evaluaties en incidentanalyse) daadwerkelijk wordt uitgevoerd en aantoonbaar wordt vastgelegd. Opnemen in jaarplanning.

15. Aantonen hoe logreview plaatsvindt, wie verantwoordelijk is voor beoordeling van de logs en hoe opvolging van afwijkingen wordt gedocumenteerd.
    Toevoeging: Niet volledig uitgewerkt is nog wie verantwoordelijk is voor de periodieke beoordeling van de logs, met welke frequentie deze beoordeling plaatsvindt en hoe de opvolging van afwijkingen wordt vastgelegd. Aanbevolen wordt dit expliciet vast te leggen in het informatiebeveiligings- of leveranciersmanagementproces.

16. Definitieve classificatie van de AI-tool schriftelijk vastleggen en opnemen in de DPIA (**Inmiddels gereed**).

17. Restrisico's expliciet laten beoordelen en accepteren door de directie en vastleggen in de DPIA (**Inmiddels gereed**).

Aanvulling ten opzichte van eerder gegeven advies:

18. Verwerkersovereenkomst Prospectief BV-Novalink (verwerker). Verwerker organiseert 1x per jaar een bewustwordingssessie voor de kennisoverdracht van kwaliteit en informatiebeveiliging. Ook voor Prospectief?

19. Wel verdient het aanbeveling de overeenkomsten periodiek te toetsen aan wijzigingen in wetgeving, subverwerkers en technische architectuur en deze op te nemen in het leveranciersmanagementproces.

20. Toevoegen aan overzicht bewaartermijnen: logs 7 jaar.

21. Aanbevolen wordt de specifieke rollen met toegang tot auditinformatie expliciet vast te leggen in de autorisatiematrix of beheerprocedures.

22. De nauwkeurigheid en betrouwbaarheid van de AI-tool worden primair bewaakt door verplichte menselijke beoordeling van alle output, aangevuld met steekproeven, gebruikersfeedback, incidentmanagement en periodieke evaluaties. De documentatie beschrijft deze controles, maar bevat geen expliciet vastgelegde testfrequentie of kwantitatieve prestatie-indicatoren. Het verdient aanbeveling deze evaluatiefrequentie en beoordelingscriteria vast te leggen in de jaarplanning of het AI-beleid.

23. Hoe wordt omgegaan met modelupdates of versie-upgrades van de onderliggende AI-diensten en hoe wordt beoordeeld of deze wijzigingen invloed hebben op de kwaliteit, betrouwbaarheid of risico's van de verwerking?

24. Ga na of het van belang is dat bevestigd kan worden dat ook de onderliggende Vertex AI-diensten van Google zijn geconfigureerd in een modus waarbij klantdata niet wordt gebruikt voor training of verbetering van foundation models.

25. Uit de beschikbare documentatie blijkt niet of aanvullende abuse monitoring of safety monitoring door de onderliggende AI-aanbieder plaatsvindt. Aanbevolen wordt dit expliciet bij Nebelus te verifiëren en de uitkomst op te nemen in het leveranciersdossier.

26. Een formeel gedocumenteerd stop- of escalatieprotocol voor de AI-toepassing is echter niet expliciet aangetroffen. Overwogen kan worden een dergelijke procedure op te nemen in het AI-beleid of incidentmanagementproces.

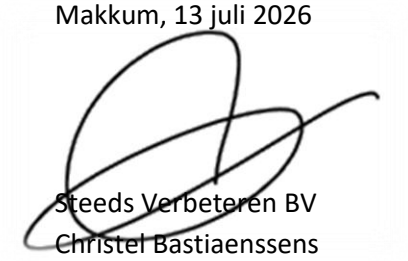
27. Overweeg vast te leggen hoe gebruikersfeedback wordt geregistreerd, beoordeeld, opgevolgd en periodiek geëvalueerd.

28. Het verdient aanbeveling om expliciet vast te leggen bij welke functionaris of afdeling gebruikers AI-gerelateerde fouten moeten melden en hoe de opvolging wordt gedocumenteerd.
    Wijs een formeel AI-contactpersoon of proceseigenaar aan voor meldingen van AI-fouten en leg dit vast in het AI-beleid of incidentproces.

Ik raad Prospectief BV aan de aanbevelingen op te nemen in het ISO-verbeterregister zodat de voortgang bewaakt wordt.

Ik dank Prospectief BV voor de gastvrijheid en openheid gedurende het DPIA-proces.

Makkum, 13 juli 2026



Steeds Verbeteren BV
Christel Bastiaenssens

RAPPORTAGE UITGEVOERDE DPIA

Deze DPIA is opgebouwd uit de door de AVG (art. 35 lid 7) voorgeschreven onderdelen:

- Systematische beschrijving van de verwerkingen en de verwerkingsdoelen
- AI-systemen en de risico's
- Algoritmen of model
- Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking
- Risicobeoordeling voor betrokkene
- Aanbeveling te treffen beheersmaatregelen (zie managementsamenvatting en conclusie)

In de bijlagen wordt ingegaan op de volgende onderwerpen: privacy principes, grondslagen, doelbinding, rechten van betrokkene, algoritme, algoritmeregister Nederlandse overheid, bias en definities.

3. Systematische beschrijving van de verwerkingen en de verwerkingsdoelen

H. Inventarisatie

1. Een korte beschrijving van de nieuwe gegevensverwerking (proces/wijziging/project/initiatief).
Het verhogen van de efficiency (verhogen kwaliteit van dossieranalyse; versnellen van beoordeling; verbeteren consistentie; verminderen administratieve belasting) door het gebruik van de AI-tool bij: • Samenvatting van medische dossiers • Identificatie van relevante medische en juridische argumenten • Conceptanalyse en rapportage ter ondersteuning van de professional • Interne kennisondersteuning (bijv. opzoeken van richtlijnen, ICF-classificatie)
2. Proceseigenaar, verantwoordelijk voor de privacy compliance van de verwerking en de eindverantwoordelijke voor deze verwerking
Proceseigenaar: Shajan Omar (Operationeel manager) Eindverantwoordelijke: Ulla Al-Saad (Algemeen Directeur)
3. Welke categorie(ën) van betrokkenen persoonsgegevens worden verwerkt? Geef daarbij aan wat de relatie is tot de betrokkenen
O : Cliënten O : Leerlingen O : Patiënten O : Medewerkers **X** : Overige, te weten: werknemers (=client/patiënt) van de klant (= werkgever) van Prospectief als (toekomstige) arbodienst en bij bezwaar en beroepsprocedures.
4. Welke categorieën van persoonsgegevens worden verwerkt?
X: Gewone persoonsgegevens, te weten: NAW, contactgegevens, leeftijd, geslacht (gepseudonimiseerd bij gebruik AI-tool) **X**: Gevoelige persoonsgegevens, te weten: mogelijk BSN (gepseudonimiseerd bij gebruik AI-tool) **X**: Bijzondere persoonsgegevens, te weten: inhoud medische dossiers O: Strafrechtelijke persoonsgegevens, te weten: …
5. Wat is de herkomst van de persoonsgegevens?
Van de werknemer (=client/patiënt) zelf, aangevuld met informatie door de bedrijfsarts (medisch dossier) inclusief (mogelijk) rapportages en correspondentie (bijv. AD-rapportages, UWV-stukken).
6. Aan welke categorieën ontvangers worden de persoonsgegevens verstrekt? Zijn deze als verwerker te kwalificeren?
Novalink (verwerker) Nebelus (subverwerker) Google Cloud Platform Europe-West 4 (subverwerker)
7. In welke landen vindt de verwerking plaats? Worden persoonsgegevens aan derde landen (= landen buiten de EER) of aan internationale organisaties doorgegeven? Zo ja, zijn er passende waarborgen, en zo ja, welke zijn dat?
Hosting: Google Cloud Platform Europe-West4 (Nederland). Nebelus is gevestigd in de Verenigde Arabische Emiraten.

Persoonsgegevens worden uitsluitend verwerkt door Prospectief BV en haar gecontracteerde verwerkers en subverwerkers. De verwerking vindt plaats binnen de Europese Economische Ruimte (EER). Er vindt volgens de overeengekomen architectuur geen toegang tot persoonsgegevens plaats vanuit landen buiten de EER. Contractueel is vastgelegd dat: • verwerking plaatsvindt binnen de EER; • systeemtoegang uitsluitend vanuit de EU plaatsvindt; • geen doorgifte naar derde landen plaatsvindt.
8. Bewaartermijnen die voor deze persoonsgegevens van toepassing zijn.
Bewaartermijnen in kaart brengen voor bronbestanden (bijv. medische dossiers, rapporten enz), chunks, embeddings, auditlogs en back-ups documenteren. Als aangegeven wordt dat bestanden verwijderd worden, dan wil je ook graag weten of ook alle bestanden uit de verwerkingsslagen (chunks, embeddings) verwijderd worden (**zie aanbeveling 6**).
9. Doel(en) van de verwerking (*meerdere antwoorden mogelijk*).
Analyseren medische dossiers, ondersteunen bezwaarprocedures, genereren van conceptanalyses, verhogen kwaliteit van beoordelingen.
10. Rechtsgrond(en) van de verwerking (*meerdere antwoorden mogelijk*) (zie bijlage 2).
Wettelijke verplichting (arbowetging), uitvoeren van de overeenkomst (met werkgevers=klanten) Gebruik AI-tool verandert deze grondslag niet. De verwerking vindt plaats onder verantwoordelijkheid van BIG-geregistreerde artsen die gebonden zijn aan het medisch beroepsgeheim. **(zie aanbeveling 2)**

NB 1) Indien vraag 9 en/of 10 niet beantwoord kan/kunnen worden, is de verwerking waarschijnlijk niet toegestaan.

NB 2) Indien de organisatie deze verwerking gaat uitvoeren en zij een verwerkingsregister moet bijhouden, dan bevatten de antwoorden van vraag 1 t/m 10 de input om dit register voor deze verwerking op te stellen of aan te vullen.

I. Analyse hoog privacyrisico

11. Is een van de drie criteria van artikel 35 lid 3 AVG van toepassing? Zo ja, welke en licht dit toe	Nee	Ja
1. Systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen;	X	
2. Op grote schaal* bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt;	X	
3. Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).	X	
* Op grote schaal: gegevens van 10.000 of meer cliënten/patiënten in één informatiesysteem.		

Uitleg begrip 'grootschalig' verduidelijkt voor alle zorgaanbieders | Autoriteit Persoonsgegevens Momenteel worden er persoonsgegevens verwerkt van 20 klanten, die gezamenlijk betrekking hebben op ongeveer 5.000 werknemers (patiënten/cliënten). De verwachting is dat het totaal van 10.000 werknemers in de nabij toekomst zal worden behaald.		
12. Is/zijn er een of meerdere categorieën van de lijst van de Autoriteit Persoonsgegevens van toepassing? Zo ja, welke en licht dit toe. (zie: Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens)	Nee	Ja
Heimelijk onderzoek, zwarte lijsten, fraudebestrijding, creditscores, financiële situatie, genetische persoonsgegevens, **gezondheidsgegevens**, samenwerkingsverbanden, cameratoezicht, controle werknemers, locatiegegevens, communicatiegegevens, internet of things, profilering, observatie en & beïnvloeding van gedrag, biometrische gegevens		X
13. Zijn er twee of meer criteria van de EDPB guidelines (richtsnoer WP248 rev.01) van toepassing?	Nee	Ja
Evaluatie of scoretoekenning, geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg, stelselmatige monitoring, **gevoelige gegevens of gegevens van zeer persoonlijke aard, op grote schaal verwerkte gegevens**, matching of samenvoeging van datasets, **gegevens met betrekking tot kwetsbare betrokkenen**, **innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen,** betrokkenen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst		X
14. Is er anderszins sprake van een dusdanig hoog privacy risico dat een DPIA nodig is? Bijvoorbeeld door gebruik van nieuwe technologieën (in combinatie met andere criteria).	Nee	Ja
AI		X

15. Beschrijf het juridische en beleidsmatige kader
Welke wet- en regelgeving is, naast de AVG en de UAVG, van toepassing op de verwerking?

- AVG/UAVG (Europese privacywetgeving)
- AI Act
- ISO9001 incl. Certificatieschema Arbodiensten (incl. Interpretatiedocument v3.0)
- NEN7510-1+A1 (informatiebeveiliging persoonlijke gezondheidsinformatie) (Prospectief BV is hier niet voor gecertificeerd maar de beheersmaatregelen genoemd in Annex A van deze norm zijn meegenomen in deze DPIA).

MDR niet van toepassing. De AI-tool wordt uitsluitend gebruikt voor **niet-medische doeleinden** zoals administratieve samenvattingen en valt niet onder de MDR (dus geen medisch hulpmiddel).

16. Hoofdstappen in woorden

1. Dossier samenstellen
Verzamelen van medische rapportages, UWV-besluiten, FML's, arbeidsdeskundige rapportages, bezwaarstukken en overige relevante documentatie.

2. Pseudonimiseren
Verwijderen van direct identificerende gegevens en toekennen van een unieke case_id.

3. Upload naar AI-platform
Aanbieden van het gepseudonimiseerde dossier aan het AI-platform van Nebelus.

4. Parsing van documenten
Omzetten van documenten naar machine-leesbare tekst.

5. Chunking
Opsplitsen van tekst in kleinere betekenisvolle tekstfragmenten (chunks).

6. Genereren van embeddings
Omzetten van chunks naar vectorrepresentaties voor semantisch zoeken.

7. AI-analyse (RAG + LLM)
Analyse van dossierinformatie en genereren van conceptanalyses en argumenten.

8. Genereren van output
Opstellen van samenvattingen, conceptadviezen en conceptonderbouwingen.

9. Menselijke beoordeling
Controle van de AI-output door een medewerker of BIG-geregistreerde arts.

10. Gebruik en verwijdering
Gebruik van de output in het primaire proces en verwijdering van tijdelijke verwerkingsdata conform afspraken.

17. Overzicht partijen, systemen en rollen
Een overzicht van de partijen, systemen en privacyrollen die onderdeel zijn van de verwerking.

Partij	Applicatie/systeem	Privacyrol	Uitleg
Prospectief	AI Tool	Verwerkingsverantwoordelijke	(toekomstige) Arbodienst, dossierhouder
NovaLink	-	Verwerker	Contractuele dienstverlening
Nebelus	AI-platform	Subverwerker	AI-modellen en beveiliging
Google Cloud Platform	Hosting	Subverwerker	In West-Europa

(zieke) Werknemer (Client/patiënt)	nvt	Betrokkene	-

18. Hoeveelheid Van hoeveel betrokkenen worden de persoonsgegevens verwerkt en wat is de omvang van de verwerkte persoonsgegevens?
De persoonsgegevens worden verwerkt van 20 klanten, die gezamenlijk betrekking hebben op ongeveer 5.000 werknemers (patiënten/cliënten).
19. Verwachting betrokkenen Verwachten betrokkenen dat hun persoonsgegevens worden verwerkt en bestaan er zorgen over deze verwerking?
De betrokkenen worden geïnformeerd over de gegevensverwerking en hun rechten. Dit wordt gedaan via een duidelijke en begrijpelijke privacyverklaring die beschikbaar is op de website en een informatiebrief die verstrekt wordt tijdens het verzamelproces.
20. Transparantie Hoe voldoet men aan de wettelijke (privacy)informatieverplichtingen tegenover betrokkenen?
Zie 19.
21. Rechten betrokkenen (zie bijlage 4) Hoe geeft men invulling aan de rechten van betrokkenen en aan privacy vragen / -verzoeken?
Men geeft invulling aan de rechten van betrokkenen en aan privacy-vragen en -verzoeken door deze rechten duidelijk toe te lichten in het privacyreglement op de website. Daarnaast is voor medewerkers van Prospectief een intern proces opgesteld waarin is vastgelegd hoe privacy-vragen en verzoeken van betrokkenen worden behandeld en afgehandeld. Bovendien is expliciet opgenomen dat een betrokkene kan verzoeken om een volledig handmatige beoordeling zonder inzet van AI. Prospectief geeft aan dat een dergelijk verzoek altijd wordt gehonoreerd.
22. Kennis & awareness Hoe wordt de (privacy) kennis van medewerkers op het benodigde niveau gehouden mbt de AI-tool?
In het interne AI-beleid is opgenomen dat medewerkers die met de AI-tool werken voldoende AI-kennis moeten bezitten en dat opleiding en instructie onderdeel zijn van het gebruik van het systeem (AI-geletterdheid) (**zie aanbeveling 13**). Verwerkersovereenkomst Prospectief BV-Novalink (verwerker). Verwerker organiseert 1x per jaar een bewustwordingssessie voor de kennisoverdracht van kwaliteit en informatiebeveiliging **(zie aanbeveling 18).**

23. Verwerkersovereenkomsten
Zijn met verwerkers verwerkersovereenkomsten afgesloten die voldoen aan de AVG-eisen? Dezelfde vraag voor (joint) controllerovereenkomsten bij (joint) controllers (= gezamenlijk verwerkingsverantwoordelijken).

Ja, Prospectief BV heeft een verwerkersovereenkomst gesloten met NovaLink B.V. en NovaLink heeft een subverwerkersovereenkomst gesloten met Nebelus Information Technology L.L.C S.O.C. De overeenkomsten bevatten de in artikel 28 AVG vereiste bepalingen, waaronder verwerking op instructie, geheimhouding, beveiligingsmaatregelen, auditrechten, ondersteuning bij betrokkenenrechten, incidentmelding en doorlegging van verplichtingen aan subverwerkers.

Wel verdient het aanbeveling de overeenkomsten periodiek te toetsen aan wijzigingen in wetgeving, subverwerkers en technische architectuur en deze op te nemen in het leveranciersmanagementproces (**zie aanbeveling 19**).

24. Autorisaties
Zijn de autorisaties ingericht op basis van '*need to know*' (*role based access*)?

Ja, volgens de documentatie zijn autorisaties ingericht op basis van role based access control (RBAC) en het need-to-know-principe. Aanvullend wordt aanbevolen deze inrichting aantoonbaar vast te leggen in een autorisatiematrix waarin rollen, bevoegdheden en toegang tot heridentificatiesleutels* zijn opgenomen **(zie aanbeveling 10).**

*Heridentificatiesleutels zijn de gegevens waarmee een gepseudonimiseerd dossier weer aan een concrete persoon kan worden gekoppeld.

25. Informatiebeveiliging
Welke (soorten) beveiligingsmaatregelen zijn getroffen bij deze verwerking? Welke specifieke beveiligingsnormen gelden er voor dit proces? Wordt daaraan voldaan?

De verwerking wordt beschermd door een combinatie van organisatorische, technische en contractuele beveiligingsmaatregelen, waaronder pseudonimisering, encryptie, MFA, RBAC, logging conform NEN7513, Confidential Computing, verwerking binnen de EER, geheimhouding, incidentmanagement en menselijk toezicht op AI-output.

Technische maatregelen:

Pseudonimisering
- Alleen gepseudonimiseerde dossiers worden verwerkt.
- Heridentificatiesleutels blijven onder beheer van Prospectief.

Encryptie
- TLS 1.3 voor datatransport.
- AES-256 encryptie voor opslag (at rest).

Authenticatie en autorisatie
- Multifactor-authenticatie (MFA).
- Role Based Access Control (RBAC).
- Need-to-know-principe.

Logging en auditing
- Logging conform NEN7513.
- Audittrail van verwerkingsactiviteiten.
- Bewaartermijn auditlogs minimaal 7 jaar (**zie aanbeveling 20).**

Confidential Computing
- Verwerking binnen Trusted Execution Environments (TEE).
- Data blijft versleuteld tijdens verwerking.

Cloudbeveiliging
- Hosting binnen Google Cloud Platform regio europe-west4 (Nederland).
- Geografische beperking van verwerking binnen de EER.

AI-specifieke maatregelen
- Geen training of finetuning op klantgegevens.
- Geen gebruik van prompts, input of output voor modelverbetering.
- Menselijke controle op alle AI-output.

26. Datalekkenbeleid
Beschikt men over een datalekkenbeleid, een effectieve procedure en een datalekkenregister

Ja, Prospectief BV beschikt over een procedure voor informatiebeveiligingsgebeurtenissen, meldplicht datalekken en een datalekkenregister.

27. Kwaliteit
Beschikt men over procedures om de kwaliteit van de gegevens te waarborgen? Dus om ervoor te zorgen dat de gegevens actueel, juist en volledig zijn en blijven.

Ja. De kwaliteit van gegevens wordt geborgd door menselijke beoordeling van AI-output, periodieke kwaliteitscontroles, gebruikersfeedback, incidentmanagement, correctiemogelijkheden voor betrokkenen en beheer van heridentificatiesleutels. Daarnaast worden AI-uitkomsten niet zonder menselijke beoordeling gebruikt. Hiermee zijn maatregelen aanwezig om de juistheid, volledigheid en actualiteit van gegevens te waarborgen.

Het AI-beleid bepaalt dat AI-output nooit zonder beoordeling wordt gebruikt.
Een medewerker of BIG-geregistreerde arts controleert de output op:
- juistheid;
- volledigheid;
- relevantie;
- eventuele hallucinaties of fouten

In het AI-beleid is opgenomen dat periodiek wordt geëvalueerd:
- kwaliteit van AI-output;
- gebruikersfeedback;
- incidenten;
- structurele afwijkingen.

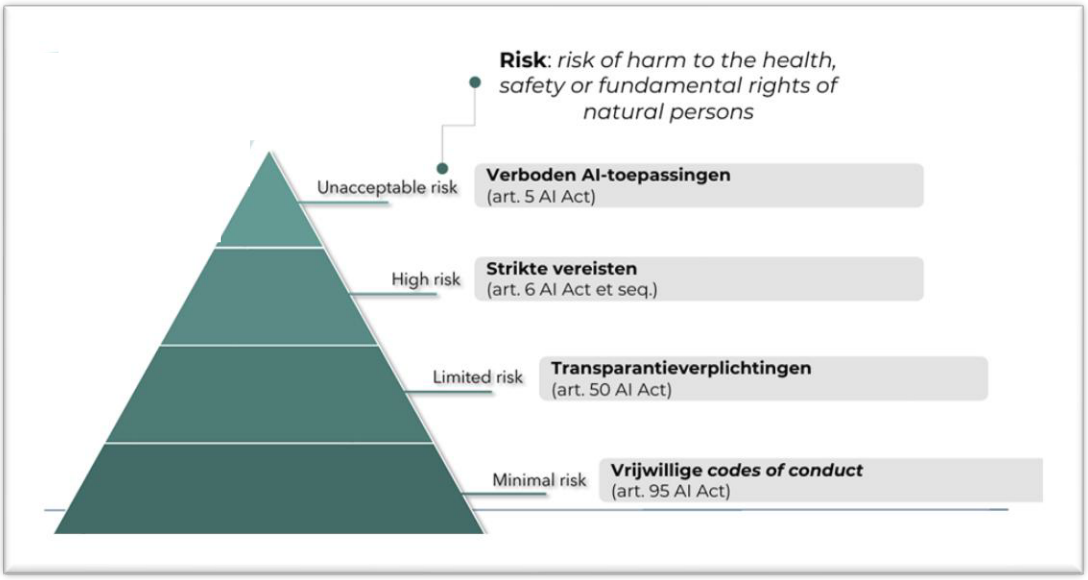
Daarnaast worden steekproeven uitgevoerd en beoordeeld.

AI-gerelateerde fouten worden geregistreerd en onderzocht.

28. Afstemming met betrokkenen
Zijn betrokkenen ten tijde van de DPIA naar hun mening gevraagd over de verwerking en is die meegenomen in de DPIA?

De volgende betrokkenen zijn meegenomen in het (pre) DPIA-proces:
Prospectief (verwerkingsverantwoordelijke)
Novalink (verwerker)
AI-gespecialiseerde jurist
Externe Functionaris Gegevensbescherming

4. AI-systemen en de risico's [2]



J. Systemen met een onaanvaardbaar risico: verboden AI

29. Onaanvaardbaar risico

Systemen die een onaanvaardbaar risico met zich meebrengen worden verboden. U mag deze systemen dus niet aanbieden of gebruiken. Dit verbod gaat februari 2025 in. Hieronder vallen bijvoorbeeld systemen en toepassingen die de vrije keuze van mensen te veel beperken, die manipuleren of die discrimineren. Denk aan systemen die worden gebruikt in of voor:

- 'social scoring' op basis van bepaald sociaal gedrag of persoonlijke kenmerken;
- 'predictive policing' om strafbare feiten bij mensen te beoordelen of te voorspellen;
- het creëren of (via scraping) uitbreiden van databanken voor gezichtsherkenning;
- manipuleren of misleiden van mensen;
- emotieherkenning in de werkomgeving en het onderwijs;
- biometrische identificatie op afstand voor rechtshandhaving. Hier zijn wel enkele uitzonderingen van toepassing; Strikte uitzonderingen zijn strikt gedefinieerd en gereguleerd, bijvoorbeeld wanneer dat nodig is om een vermist kind op te sporen, om een specifieke en onmiddellijke terroristische dreiging te voorkomen of om een dader of verdachte van een ernstig strafbaar feit op te sporen, te lokaliseren, te identificeren of te vervolgen.
  Dit gebruik is onderworpen aan de toestemming van een rechterlijke of andere onafhankelijke instantie en aan passende beperkingen in de tijd, het geografische bereik en de doorzochte databanken.
- biometrische categorisering, waarbij mensen op basis van biometrische gegevens in bepaalde gevoelige categorieën worden ingedeeld.

[2] Geraadpleegde bronnen:

- Risicogroepen AI-verordening | Autoriteit Persoonsgegevens
- Artificial Intelligence – Q&As (europa.eu)
- AI-verordening AI (Artificiële Intelligentie) - Digitale Overheid
- De impact van de EU AI Act: Responsible AI en inzichten van de EU AI Barometer | EY - Nederland

Wordt gebruik gemaakt van dergelijke systemen?
O: Ja. Stop met het verder invullen van de DPIA en stop met het aanbieden of gebruiken van een dergelijk systeem.
X: Nee, ga verder naar de volgende vraag.

K. Systemen met een hoog risico

30. Hoog risico
Voor AI-systemen die vallen in de risicogroep 'hoog risico' gelden strikte verplichtingen. Wanneer u daar niet aan kunt voldoen, mag u het systeem niet in de handel brengen of gebruiken.

De verplichtingen voor dit soort systemen gaan gelden vanaf augustus 2026. Denk aan AI-systemen die worden gebruikt in of voor:

- kritieke infrastructuur (vervoer, levering van water, gas, verwarming en elektriciteit), die het leven en de gezondheid van burgers in gevaar kan brengen;
- veiligheidscomponenten van producten (bv. AI-toepassing in robotgeassisteerde chirurgie);
- onderwijs of beroepsopleiding, waarbij het systeem de toegang tot het onderwijs en de loop van iemands beroepsleven kan bepalen. Bijvoorbeeld het beoordelen van examens;
- werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid, onder andere vanwege de aanzienlijke risico's voor toekomstige carrièrekansen en het levensonderhoud van mensen. Bijvoorbeeld een AI-systeem dat automatisch cv's selecteert voor de volgende ronde in een wervingsprocedure;
- essentiële particuliere en openbare diensten. Zulke systemen kunnen grote effecten hebben op bijvoorbeeld het levensonderhoud van mensen. Bijvoorbeeld software die bepaalt wanneer iemand wel of geen uitkering of lening krijgt;
- rechtshandhaving, omdat dit afbreuk kan doen aan de grondrechten van mensen. Bijvoorbeeld een AI-systeem dat wordt gebruikt voor de beoordeling van de betrouwbaarheid van bewijsmateriaal;
- toegang tot essentiële particuliere en publieke diensten en uitkeringen (bijvoorbeeld gezondheidszorg), de beoordeling van de kredietwaardigheid van natuurlijke personen, en risicobeoordeling en prijsstelling met betrekking tot levens- en ziektekostenverzekeringen;
- migratie, asiel en grenzen. Bijvoorbeeld geautomatiseerde behandeling van asielaanvragen;
- rechtsbedeling en democratische processen, omdat het gebruik hiervan risico's kent voor de democratie en de rechtsstaat. Bijvoorbeeld een AI-systeem dat ondersteunt bij rechterlijke uitspraken.
- Verdere verplichtingen kunnen worden gespecificeerd in latere AI-regelgeving voor de gezondheidszorg, financiële dienstverlening, automobiel-, luchtvaart- en andere sectoren.

Valt het systeem dat u wilt aanbieden of inzetten in de categorie 'hoog risico?' Dan gelden er regels om deze risico's te voorkomen of te beperken tot een aanvaardbaar niveau. Bijvoorbeeld regels over risicobeheer, de kwaliteit van de gebruikte data, technische documentatie en registratie, transparantie en menselijk toezicht. Overheden of uitvoerders van publieke taken moeten bij systemen met een hoog risico een 'grondrechteneffectbeoordeling' doen.

Wordt gebruik gemaakt van dergelijke systemen? O: Ja. Dan gelden er regels om deze risico's te voorkomen of te beperken tot een aanvaardbaar niveau (zie alinea hierboven). Ga verder naar vraag 33. **X** : Nee, ga verder naar de volgende vraag.

L. Systemen met een beperkt risico

31. Beperkt risico Voor AI-toepassingen met een beperkt risico geldt een aantal transparantieverplichtingen. Het gaat om AI-systemen die bedoeld zijn om met personen in contact te komen, zoals chatbots. En AI-systemen die zelf inhoud maken, zoals teksten en beeldmateriaal. Als u deze systemen aanbiedt of gebruikt, dan moet u mensen erover informeren dat zij met AI te maken hebben. Deze transparantieverplichtingen gaan gelden vanaf augustus 2026.
Wordt gebruik gemaakt van systemen met een beperkt risico? **X** : **Ja. Hiervoor geldt een aantal transparantieverplichtingen. Als u deze systemen aanbiedt of gebruikt, dan moet u mensen erover informeren dat zij met AI te maken hebben.** O: Nee, ga verder naar de volgende vraag.

M. Systemen met een laag risico

32. Laag risico: Voor de meeste AI-toepassingen, zoals spamfilters en videogames, gelden geen specifieke wettelijke vereisten.
Wordt gebruik gemaakt van systemen met een laag risico? O: Ja. Hiervoor gelden geen specifieke wettelijke vereisten. Ga verder met invullen bij Hoofdstuk 7 Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking. **X** : Nee. Ga verder met invullen bij Hoofdstuk 7 Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking.

N. Systemen aan te merken als medisch hulpmiddel

33. MDR Is de AI-toepassing aan te merken als medisch hulpmiddel onder de MDR (CE-markering).
MDR van toepassing? O: Ja, want de software wordt gebruikt voor medische doeleinden zoals diagnose, behandeling en/of monitoring. Dit is een systeem met een hoog risico. Stop met het verder invullen van de DPIA en raadpleeg een deskundige i.v.m. het voldoen aan de MDR. **X** : Nee, ga verder met invullen bij Hoofdstuk 6 Algoritmen of model.

5. Algoritmen of model (eventueel aanbieder betrekken bij dit hoofdstuk)

O. Doel

34. Wat probeert het algoritme of het model te bereiken?
De AI-tool ondersteunt medewerkers bij de analyse van gepseudonimiseerde medische dossiers door relevante informatie te identificeren, samen te vatten en conceptmatige analyses te genereren. Het doel is het efficiënter verwerken van omvangrijke dossiers en het ondersteunen van medische advisering en bezwaar- en beroepsprocedures. Het systeem neemt geen geautomatiseerde besluiten; alle output wordt beoordeeld door een menselijke professional voordat deze wordt gebruikt.
35. Is het doel duidelijk gedefinieerd?
Het doel is duidelijk gedefinieerd. De AI-tool wordt ingezet ter ondersteuning van de analyse van gepseudonimiseerde medische dossiers, het opstellen van samenvattingen en conceptanalyses en het ondersteunen van medische advisering en bezwaar- en beroepsprocedures. Het systeem heeft uitsluitend een ondersteunende functie en neemt geen geautomatiseerde besluiten.
36. Is het doel ethisch verantwoord?
Ja. Het doel van de verwerking wordt als ethisch verantwoord beoordeeld. De AI-tool wordt uitsluitend ingezet ter ondersteuning van professionals bij de analyse van medische dossiers en bezwaar- en beroepsprocedures. Het systeem neemt geen zelfstandige beslissingen en vervangt geen medisch of juridisch oordeel. Door toepassing van pseudonimisering, menselijk toezicht, transparantie richting betrokkenen en het verbod op gebruik van gegevens voor modeltraining zijn passende ethische waarborgen getroffen.

P. Werking

37. Wat is de logica of het model dat het algoritme volgt?
De AI-tool maakt gebruik van een Retrieval Augmented Generation (RAG)-architectuur in combinatie met een Large Language Model (LLM). Documenten worden geparseerd, gechunkt en omgezet naar embeddings. Op basis van een vraag worden relevante tekstfragmenten geselecteerd en aangeboden aan het model, dat vervolgens samenvattingen, analyses of conceptteksten genereert. De gegenereerde output dient uitsluitend ter ondersteuning van medewerkers en wordt altijd beoordeeld door een menselijke professional. Er vindt geen geautomatiseerde besluitvorming plaats.
38. Welke data gebruikt het om tot een beslissing/conclusie te komen?
De AI-tool gebruikt uitsluitend gepseudonimiseerde dossierinformatie die door Prospectief wordt aangeleverd, waaronder medische rapportages, arbeidsdeskundige rapportages, UWV-documenten en bezwaar- en beroepsstukken. Deze gegevens worden verwerkt via parsing, chunking en embeddings waarna relevante informatie wordt geselecteerd voor analyse door het

taalmodel. Er worden geen externe databronnen geraadpleegd en de gegevens worden niet gebruikt voor training of finetuning van AI-modellen. De uiteindelijke conclusie of beslissing wordt altijd genomen door een menselijke professional.

Q. Data

39. Is de data representatief voor de populatie waarop het algoritme toegepast wordt?
Ja. De AI-tool gebruikt primair de door Prospectief aangeleverde dossierinformatie van de betreffende betrokkene. De gegevens waarop analyses worden gebaseerd zijn daarmee direct afkomstig uit de populatie waarop het systeem wordt toegepast. Het systeem maakt geen gebruik van een afzonderlijke, door Prospectief samengestelde trainingsdataset voor besluitvorming. Wel wordt onderkend dat het onderliggende taalmodel generiek is getraind, waardoor risico's op bias of onjuiste interpretaties kunnen bestaan. Deze risico's worden beperkt door menselijk toezicht, kwaliteitscontroles en periodieke evaluaties.
40. Zijn er biases of vooroordelen aanwezig in de data?
Er zijn geen concrete aanwijzingen dat de gebruikte dossiergegevens systematische bias bevatten. Wel wordt onderkend dat bias of vooringenomenheid in de output van het onderliggende taalmodel niet volledig kan worden uitgesloten. Dit risico wordt beperkt door menselijk toezicht, kwaliteitscontroles, incidentmanagement en het feit dat geen geautomatiseerde besluitvorming plaatsvindt. Bias en discriminatie zijn bovendien expliciet opgenomen als AI-incidentcategorieën binnen het AI-beleid.
41. Hoe is de data verzameld en is dit op een ethisch verantwoorde manier vergaard?
De gegevens zijn verzameld in het kader van de reguliere dienstverlening van Prospectief, waaronder arbodienstverlening, medische advisering en bezwaar- en beroepsprocedures. De gegevens zijn niet specifiek verzameld voor het trainen of ontwikkelen van AI-modellen. Betrokkenen worden geïnformeerd via de privacyverklaring en cliëntinformatiebrief. Voor verwerking binnen de AI-tool worden de gegevens gepseudonimiseerd en uitsluitend gebruikt ter ondersteuning van menselijke professionals. Op basis hiervan wordt de wijze van gegevensverzameling als rechtmatig en ethisch verantwoord beoordeeld.
42. Bestaat de kans op overfitting? (van toepassing bij voorspellen of classificeren)
Nee. De AI-tool maakt gebruik van een bestaande Large Language Model-omgeving en een RAG-architectuur. Er vindt geen training, finetuning of hertraining plaats op de gegevens van Prospectief. Hierdoor is het risico op overfitting, zoals dat voorkomt bij voorspellende of classificerende machine learning-modellen, niet of nauwelijks van toepassing. Voor deze verwerking zijn risico's zoals hallucinaties, bias en onjuiste interpretaties relevanter dan overfitting.
43. Bestaat de kans op onderfitting? (van toepassing bij voorspellen of classificeren)
Nee. Onderfitting is een risico dat voornamelijk voorkomt bij getrainde voorspellende of classificerende modellen. Omdat de AI-tool geen eigen model traint of finetunet op gegevens van Prospectief, is dit risico niet of nauwelijks van toepassing. Relevanter zijn risico's zoals onvolledige

analyses, hallucinaties en onjuiste interpretaties van dossierinformatie. Deze worden beperkt door menselijk toezicht en kwaliteitsborgingsmaatregelen.

R. Biases

44. Kan het algoritme discriminatie in de hand werken of versterken?
Het risico bestaat theoretisch, wordt onderkend in de documentatie en wordt gemitigeerd door menselijk toezicht, kwaliteitscontroles en het ontbreken van geautomatiseerde besluitvorming.
45. Welke maatregelen zijn genomen om biases te identificeren en te corrigeren?
Mogelijke bias wordt primair geïdentificeerd door menselijke beoordeling, kwaliteitscontroles, gebruikersfeedback en incidentmanagement. Bias en discriminatie zijn expliciet opgenomen als AI-incidentcategorieën. Geconstateerde afwijkingen kunnen worden gecorrigeerd voordat de output wordt gebruikt.

S. Transparantie

46. Kunnen de beslissingen of uitkomsten van het algoritme worden verklaard en begrepen?
Ja, grotendeels. De gebruikte RAG-architectuur maakt inzichtelijk welke dossierinformatie aan de analyse ten grondslag ligt. Gebruikers kunnen doorgaans begrijpen welke informatie uit het dossier is gebruikt voor de gegenereerde output. De exacte interne werking van het onderliggende Large Language Model is echter niet volledig uitlegbaar. Dit wordt ondervangen door menselijk toezicht, kwaliteitscontroles en het ontbreken van geautomatiseerde besluitvorming.
47. Is er documentatie of uitleg beschikbaar over hoe het algoritme werkt?
Ja. Er is uitgebreide documentatie beschikbaar over de technische en organisatorische werking van de AI-tool, waaronder de architectuur, gegevensstromen, beveiligingsmaatregelen, privacymaatregelen, menselijk toezicht, incidentmanagement en de rol van betrokken verwerkers en subverwerkers. De exacte interne werking van het onderliggende Large Language Model is niet volledig inzichtelijk, maar de toepassing en het gebruik binnen de verwerking zijn voldoende gedocumenteerd voor de beoogde inzet.
48. Worden loggings vastgelegd en periodiek beoordeeld? Door wie?
Ja. Logging en audittrails worden vastgelegd conform NEN7513 en omvatten onder meer gebruikersidentiteit, tijdstempels, uitgevoerde acties, geraadpleegde resources en toegangsgegevens. De documentatie beschrijft tevens incidentmanagement en auditlogging. Niet volledig uitgewerkt is nog wie verantwoordelijk is voor de periodieke beoordeling van de logs, met welke frequentie deze beoordeling plaatsvindt en hoe de opvolging van afwijkingen wordt vastgelegd. Aanbevolen wordt dit expliciet vast te leggen in het informatiebeveiligings- of leveranciersmanagementproces (**zie aanbeveling 15).**

49. Wordt een Audit Trail vastgelegd en wie hebben hier toegang toe?
Ja. Er wordt een audit trail vastgelegd. De audit trail bevat onder meer gebruikersidentiteit, tijdstempels, uitgevoerde acties, geraadpleegde resources en toegangsgegevens. De auditinformatie wordt bewaard voor audit-, beveiligings- en incidentonderzoeksdoeleinden. Toegang tot de audit trail is beperkt via role based access control (RBAC), MFA en het need-to-know-principe. Aanbevolen wordt de specifieke rollen met toegang tot auditinformatie expliciet vast te leggen in de autorisatiematrix of beheerprocedures (**zie aanbeveling 21).**

T. Gevolgen gebruik algoritme

50. Wat is de mogelijke impact op individuen en gemeenschappen, zowel positief als negatief?
Positieve impact De inzet van de AI-tool kan bijdragen aan: • efficiëntere verwerking van omvangrijke medische dossiers; • snellere identificatie van relevante informatie; • consistentere dossieranalyse; • ondersteuning van medische professionals bij bezwaar- en beroepsprocedures; • vermindering van administratieve belasting; • betere toegankelijkheid van dossierinformatie; • verbeterde kwaliteit van de voorbereiding van medische adviezen. Hierdoor kunnen cliënten mogelijk sneller en beter worden geholpen. Het systeem ondersteunt professionals bij het verwerken van grote hoeveelheden informatie en kan relevante informatie inzichtelijk maken die anders mogelijk minder snel wordt gevonden. **Negatieve impact** Mogelijke negatieve gevolgen zijn: • onjuiste of onvolledige AI-output (hallucinaties); • verkeerde interpretatie van medische informatie; • risico op bias of vooringenomenheid in de output; • verlies van vertrouwen indien AI-uitkomsten onjuist blijken; • privacyrisico's vanwege verwerking van gezondheidsgegevens; • risico dat gebruikers te veel vertrouwen op AI-gegenereerde analyses; • mogelijke onjuiste ondersteuning van medische advisering indien menselijke controle tekortschiet. De verwerking richt zich primair op individuele dossiers en niet op groepen of gemeenschappen.
51. Welke onbedoelde gevolgen kunnen optreden?
Mogelijke onbedoelde gevolgen zijn onder meer onjuiste of onvolledige AI-output, automation bias, vooringenomenheid in gegenereerde teksten, privacy-incidenten, afhankelijkheid van AI en onjuiste interpretatie van output. Deze risico's worden beperkt door menselijk toezicht, kwaliteitscontroles, incidentmanagement, pseudonimisering en het ontbreken van geautomatiseerde besluitvorming.

U. Nauwkeurigheid en betrouwbaarheid

52. Welke methoden worden gebruikt om de prestaties van het algoritme te evalueren?
De prestaties van de AI-tool worden beoordeeld door menselijke beoordeling van output, steekproeven, gebruikersfeedback, incidentanalyse en periodieke evaluaties.
53. Hoe vaak en op welke manier wordt de AI-tool getest op nauwkeurigheid en betrouwbaarheid?
De nauwkeurigheid en betrouwbaarheid van de AI-tool worden primair bewaakt door verplichte menselijke beoordeling van alle output, aangevuld met steekproeven, gebruikersfeedback, incidentmanagement en periodieke evaluaties. De documentatie beschrijft deze controles, maar bevat geen expliciet vastgelegde testfrequentie of kwantitatieve prestatie-indicatoren. Het verdient aanbeveling deze evaluatiefrequentie en beoordelingscriteria vast te leggen in de jaarplanning of het AI-beleid **(zie aanbeveling 22).**
54. Hoe vaak wordt het algoritme geüpdatet of opnieuw getraind?
Er vindt geen hertraining of finetuning plaats op gegevens van Prospectief. Het systeem leert niet van de verwerkte dossiers. Eventuele updates hebben betrekking op de applicatie, beveiliging of onderliggende AI-diensten van de leverancier. Hoe wordt omgegaan met modelupdates of versie-upgrades van de onderliggende AI-diensten en hoe wordt beoordeeld of deze wijzigingen invloed hebben op de kwaliteit, betrouwbaarheid of risico's van de verwerking? **(zie aanbeveling 23).**
55. Hoe wordt model drift tegengegaan?
Klassieke model drift wordt beperkt doordat geen training of finetuning plaatsvindt op gegevens van Prospectief. Mogelijke kwaliteitsveranderingen als gevolg van updates van het onderliggende AI-model worden ondervangen door menselijk toezicht, steekproeven, gebruikersfeedback, incidentmanagement en periodieke evaluaties.

V. Privacy en veiligheid van gegevens

56. Hoe wordt omgegaan met de persoonlijke informatie die door het algoritme wordt verwerkt?
Persoonlijke informatie wordt vooraf gepseudonimiseerd, uitsluitend verwerkt voor de overeengekomen doeleinden en beschermd door passende technische en organisatorische maatregelen. De gegevens worden niet gebruikt voor training of verbetering van AI-modellen. Toegang is beperkt op basis van het need-to-know-principe en betrokkenen kunnen gebruikmaken van hun AVG-rechten, waaronder inzage, correctie en verwijdering. Verwijdering van gegevens omvat tevens de onderliggende opslaglagen zoals embeddings.
57. Zijn er maatregelen genomen om gegevensinbreuken (schending) te voorkomen?

Ja. Er zijn passende technische, organisatorische en contractuele maatregelen getroffen om gegevensinbreuken te voorkomen. Deze omvatten onder meer pseudonimisering, encryptie, MFA, role based access control, need-to-know autorisaties, logging conform NEN7513, audittrails, verwerking binnen de EER, geheimhoudingsverplichtingen, leveranciersbeheer en incidentmanagement. Daarnaast zijn procedures ingericht voor detectie, registratie en afhandeling van beveiligingsincidenten en datalekken.
58. Is met aanbieder (bijv. Microsoft) contractueel vastgelegd dat zij geen prompts en user input gaan gebruiken?
Ja. In de verwerkersovereenkomst en subverwerkersovereenkomst is expliciet vastgelegd dat persoonsgegevens, prompts, input en output niet worden gebruikt voor training, finetuning of verbetering van AI-modellen. De verwerking is beperkt tot de overeengekomen dienstverlening. Hiermee is contractueel geborgd dat de verwerkte gegevens niet worden ingezet voor verdere ontwikkeling van AI-modellen. Ga na of het van belang is dat bevestigd kan worden dat ook de onderliggende Vertex AI-diensten van Google zijn geconfigureerd in een modus waarbij klantdata niet wordt gebruikt voor training of verbetering van foundation models (**zie aanbeveling 24).**
59. Is er een aanvraag ingediend bij bijv. Microsoft die zorgt dat abuse monitoring wordt uitgeschakeld **(Abuse monitoring is een check die automatisch plaatsvindt op het moment dat de prompt naar het AI-model wordt gestuurd. Als er misbruik gedetecteerd wordt, dan worden de system prompt en de user input tijdelijk opgeslagen om gereviewed te worden door bijv. Microsoft. Zij controleren of AI is gebruikt voor illegale praktijken (abuse).** Link: Azure OpenAI Limited Access Review: Modified Abuse Monitoring (via de eigen organisatie indienen en niet via ICT-leverancier)
Niet vastgesteld. Uit de beschikbare documentatie blijkt niet of aanvullende abuse monitoring of safety monitoring door de onderliggende AI-aanbieder plaatsvindt. Aanbevolen wordt dit expliciet bij Nebelus te verifiëren en de uitkomst op te nemen in het leveranciersdossier (**zie aanbeveling 25).**

W. Aanpassen of stoppen indien nodig

60. Is er een mechanisme om het algoritme aan te passen als het niet goed functioneert?
Ja. De organisatie beschikt over mechanismen om het gebruik van de AI-tool aan te passen wanneer kwaliteitsproblemen, hallucinaties, bias, modelafwijkingen of andere AI-incidenten worden vastgesteld. Afwijkingen kunnen worden gesignaleerd via menselijke beoordeling, gebruikersfeedback, steekproeven, incidentmanagement en periodieke evaluaties. Op basis hiervan kunnen prompts, werkinstructies of het gebruik van de AI-functionaliteit worden aangepast. Daarnaast kan het gebruik van de AI-tool indien nodig worden beperkt of tijdelijk worden opgeschort.
61. Kan het gebruik van het algoritme eenvoudig worden stopgezet als het schadelijk blijkt te zijn?
Ja. Het gebruik van de AI-tool kan relatief eenvoudig worden stopgezet. De toepassing ondersteunt bestaande werkprocessen maar vervangt deze niet Het gebruik van de AI-tool kan worden gestaakt doordat de organisatie kan terugvallen op handmatige processen. Een formeel gedocumenteerd stop- of escalatieprotocol voor de AI-toepassing is echter niet expliciet aangetroffen. Overwogen kan worden een dergelijke procedure op te nemen in het AI-beleid of incidentmanagementproces (**zie aanbeveling 26**).

X. Gebruikers

62. Hoe worden medewerkers getraind in het gebruik van deze AI-tool?
Medewerkers worden geïnstrueerd over verantwoord gebruik van de AI-tool via het AI-beleid, bewustwordingsactiviteiten, privacy- en informatiebeveiligingsmaatregelen en de verplichting tot menselijke beoordeling van AI-output. Daarnaast gelden geheimhoudingsverplichtingen en het afgeleid medisch beroepsgeheim. De documentatie bevat echter nog geen volledig uitgewerkt opleidingsprogramma met aantoonbare registratie van gevolgde trainingen, deelnemers en herhalingsmomenten. Aanbevolen wordt dit vast te leggen in het kader van AI-geletterdheid en compliance met de AI Act (**zie aanbeveling 13**).
63. Hoe wordt feedback van gebruikers verzameld en verwerkt om de tool te verbeteren?
Feedback van gebruikers wordt verzameld via kwaliteitscontroles, gebruikerservaringen, incidentmeldingen en evaluaties van AI-output. Deze feedback wordt gebruikt voor het verbeteren van processen, werkinstructies, kwaliteitscontroles en beheersmaatregelen rondom de AI-toepassing. Overweeg vast te leggen hoe gebruikersfeedback wordt geregistreerd, beoordeeld, opgevolgd en periodiek geëvalueerd (**zie aanbeveling 27).**

64. Wat gebeurt er als gebruikers niet tevreden zijn met de uitkomst die door de AI is gegenereerd?
Wanneer gebruikers niet tevreden zijn met de AI-output, kunnen zij deze corrigeren, negeren of vervangen door een handmatige analyse. De AI-output wordt niet automatisch overgenomen en de eindverantwoordelijkheid blijft bij de menselijke professional. Bij structurele kwaliteitsproblemen worden incidentmanagement en evaluatieprocessen ingezet. Betrokkenen kunnen daarnaast verzoeken om een volledig menselijke beoordeling.

Y. Verantwoordelijkheid

65. Wie draagt de verantwoordelijkheid voor de beslissingen die door het algoritme worden genomen?
Het algoritme neemt geen besluiten. Het systeem genereert uitsluitend ondersteunende analyses, samenvattingen en conceptteksten. De uiteindelijke beoordeling en eventuele medische, arbeidsdeskundige of juridische conclusies worden uitsluitend genomen door een menselijke professional. De verantwoordelijkheid voor de uitkomst ligt niet bij het algoritme, maar bij de menselijke gebruiker die de AI-output beoordeelt en gebruikt. Prospectief blijft als verwerkingsverantwoordelijke eindverantwoordelijk voor de verwerking van persoonsgegevens en de gevolgen van het gebruik van de AI-tool.
66. Is er een aanspreekpunt of een proces voor wanneer het algoritme fouten maakt?
Ja. Er is een AI-incidentmanagementproces aanwezig voor het melden, registreren, onderzoeken en opvolgen van AI-gerelateerde fouten, waaronder hallucinaties, bias, modelafwijkingen en kwaliteitsproblemen. Daarnaast zijn algemene incident- en datalekprocedures ingericht. Het verdient aanbeveling om expliciet vast te leggen bij welke functionaris of afdeling gebruikers AI-gerelateerde fouten moeten melden en hoe de opvolging wordt gedocumenteerd. Wijs een formeel AI-contactpersoon of proceseigenaar aan voor meldingen van AI-fouten en leg dit vast in het AI-beleid of incidentproces **(zie aanbeveling 28**).

Z. Vereisten voor systemen met een hoog risico

67. Vereisten voor aanbieders

1. Risicobeheersysteem vaststellen, uitvoeren en documenteren (art. 9 AI Act).
2. Vaststellen en analyseren van redelijkerwijs te voorziene risico's van de AI-tool en vaststellen van gepaste en gerichte risicobeheersmaatregelen.
3. Zorg voor technische documentatie van de risico's en risicobeheersmaatregelen (art. 11 AI Act) Documentatie onderhouden en bijwerken, ook na productrelease (art. 18 AI Act).
4. Beheren van data en datagovernance (art. 10 en 16(a) AI Act).
5. Data selectie: zorg ervoor datasets voor training, validatie en tests relevant, voldoende representatief, en zoveel mogelijk foutenvrij en volledig met het oog op het beoogde doel zijn.
6. Robuuste data management: relevante verwerkingsactiviteiten voor datavoorbereiding, zoals annotatie, labelen, opschoning, actualisatie, verrijking en aggregatie.
7. Om de opsporing en correctie van vertekeningen te waarborgen in relatie tot AI systemen met een hoog risico mogen de aanbieders uitzonderlijk bijzondere categorieën persoonsgegevens verwerken als passende waarborgen worden geboden.
8. Prestatie en veiligheid bewaken: corrigerende maatregelen treffen voor system.
9. Logs bewaren op een automatische en gedocumenteerde wijze (art. 12, 16(a en e) en 19 AI Act) (bijv. input en output moeten traceerbaar zijn).
10. Zorgen voor AI-bewustzijn om AI-geletterdheid te bevorderen (art. 4 AI Act). Handreiking AP: https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid
11. Zorgen voor transparantie over de aanbieder en hoe het systeem is gebouwd, en het verstrekken van gebruiksinstructies voor de gebruiksverantwoordelijke (art. 13 AI Act).
12. Beknopt, volledig, juist en duidelijk.
13. Informatie is relevant, toegankelijk en begrijpelijk voor gebruiksverantwoordelijken, bijv. systeemonderhoud, mogelijkheden en beperkingen.
14. Voldoet aan toegankelijkheidseisen (art. 16(l) AI Act).
15. AI-systeem is zodanig ontworpen en ontwikkeld dat menselijk toezicht mogelijk is (art. 14 AI Act).
16. Mensen moeten in staat worden gesteld om de capaciteiten en beperkingen te begrijpen, output juist te interpreteren, en niet te gebruiken.
17. Cyberbeveiliging (art. 15 and 16(a) AI Act).
18. Zorg voor nauwkeurigheid, robuustheid en cyberbeveiliging.
19. Zorg voor consistente performance en weerbaarheid tegen cyberbeveiligingsrisico’s.
20. Creëer een kwaliteitsbeheersysteem (art. 16(c) en 17 AI Act).
    - Kwaliteitsbeheersysteem moet bestaan uit schriftelijke beleidslijnen, procedures en instructies, bijv. het includeren van een strategie voor naleving van regelgeving en post-market monitoring.
21. Conformiteitsbeoordeling (art. 43 AI Act).
22. Conformiteitsbeoordeling (CA): stel conformiteitsverklaring op.
23. Brengen een CE-markering aan op de AI-tool.
24. Registreer AI-systeem in EU-databank voorafgaand aan in handel brengen (art. 49, 60(4c) & 70 AI Act).
25. Meld ernstige incidenten zoals bedoeld in art. 3(49) aan de toezichthoudende autoriteit (art. 73 AI Act), neem noodzakelijke corrigerende maatregelen en informeer relevante partijen (art. 16(j) and 20 AI Act).

O: Ja, wij zijn aanbieder van systemen met een hoog risico en voldoen aan het bovenstaande.
O: Ja, wij zijn aanbieder van systemen met een hoog risico en voldoen niet aan het bovenstaande.
X: Nee, wij zijn geen aanbieder van systemen met een hoog risico.

68. Vereisten voor gebruikersverantwoordelijken

1. Inzetten volgens de gebruiksinstructie (art. 26(1) AI Act).
2. Zorg ervoor dat de input relevant is voor het gebruik van het systeem (art. 26(4) AI Act).
3. Het menselijk toezicht toewijzen aan de juiste personen (art. 26(2) AI Act).
4. Informeer individuen wanneer ze mogelijk worden onderworpen aan het gebruik van AI met een hoog risico (art. 26(11) AI Act). Als er werknemers bij betrokken zijn, moeten de werknemersvertegenwoordigers worden geïnformeerd (art. 26(7) AI Act).
5. Zorg voor AI-bewustzijn om AI-geletterdheid te bevorderen (art. 4 AI Act). Handreiking AP: https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid
6. Bewaar automatisch gegenereerde logs ten minste 6 maanden, tenzij anders vereist door lokale EU wetgeving (art. 26(6) AI Act).
7. AI-systemen monitoren en het gebruik ervan onderbreken als er een risico kan ontstaan voor de gezondheid of veiligheid, of voor de grondrechten, van personen (zoals gedefinieerd in art. 79(1) AI Act en informeer de aanbieder en de markttoezichtautoriteit (art. 26(5) AI Act)
8. Aanbieder en markttoezichthouder informeren over geïdentificeerde risico's zoals bedoeld in art. 79(1) AI Act; verdere informatieplichten kunnen van toepassing zijn, bijv. in het geval van een ernstig incident (art. 26(5) AI Act).
9. Data Protection Impact Assessments (DPIA's): Waar van toepassing, gebruik informatie van de aanbieder om DPIA's uit te voeren (art. 26(9) AI Act).
10. Voor overheidsinstanties etc. (art. 26(8) AI Act): verifieer of het system is opgenomen in de EU-databank voor hoog risico AI-systemen.
11. Voer een beoordeling van de gevolgen voor de grondrechten uit voordat de AI-tool in gebruik wordt genomen (o.a. voor diensten van algemeen belang zoals banken, scholen, ziekenhuizen en verzekeraars) (art. 27 AI Act). De gebruiksverantwoordelijke kan zich baseren op dergelijke beoordelingen of DPIA's uitgevoerd door de aanbieder (art. 27(2) AI Act).
12. Werk samenwerken met relevante bevoegde autoriteiten (art. 26(12) AI Act).

O: Ja, wij zijn gebruikersverantwoordelijke van systemen met een hoog risico en voldoen aan het bovenstaande.
O: Ja, wij zijn gebruikersverantwoordelijke van systemen met een hoog risico en voldoen niet aan het bovenstaande.
X : Nee, wij zijn geen gebruikersverantwoordelijke van systemen met een hoog risico.

AA. Vereisten voor systemen met een beperkt risico

69. Vereisten voor aanbieders (art. 4 en 50(1-2) AI Act).

Transparantieverplichtingen

- Personen informeren dat zij interacteren met een AI-systeem (bijv. informeren over AI-chatbots).
- Ervoor zorgen dat outputs van AI-systemen die synthetische audio-, beeld-, video- of tekstinhoud genereren, markeren in een machineleesbaar formaat, en detecteerbaar zijn als kunstmatig gegenereerd of gemanipuleerd.
- De verplichting van AI-geletterdheid wordt tevens omschreven in hoofdstuk 1, art 4. AI-geletterdheid (m.i.v. 2-2-2025):
  'Aanbieders en gebruikers van AI-systemen dienen maatregelen te nemen om, naar beste vermogen, een voldoende niveau van AI-geletterdheid te waarborgen bij hun personeel en andere personen die betrokken zijn bij de exploitatie en het gebruik van AI-systemen namens hen. Hierbij moet rekening worden gehouden met hun technische kennis, ervaring, opleiding en training, de context waarin de AI-systemen worden ingezet, en de personen of groepen personen waarop de AI-systemen van toepassing zijn.'
  Het is voor organisaties van cruciaal belang om nu al wel maatregelen te nemen om ervoor te zorgen dat iedereen voldoende kennis heeft om met AI-systemen te werken. Hoewel het vereiste niveau van AI-geletterdheid kan variëren afhankelijk van specifieke taken en toepassingen, moeten alle medewerkers die met AI-systemen werken beschikken over enkele kerncompetenties. De belangrijkste hiervan zijn:
  a. AI herkennen: Het vermogen om AI-toepassingen te herkennen en inzicht te krijgen in hoe deze in het dagelijks leven worden gebruikt
  b. AI begrijpen: Begrip van de basisconcepten van AI, zoals machine learning en taalmodellen, en het onderscheiden van verschillende soorten AI en hun toepassingen.
  c. Praktisch gebruik: Vaardigheden om AI-tools effectief toe te passen in diverse contexten.
  d. Kritische evaluatie: Bewustzijn van de ethische vraagstukken en de maatschappelijke impact van AI.
  Handreiking AP: https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid

O: Ja, wij zijn aanbieder van systemen met een beperkt risico en voldoen aan het bovenstaande.
O: Ja, wij zijn aanbieder van systemen met een beperkt risico en voldoen niet aan het bovenstaande.
X: Nee, wij zijn geen aanbieder van systemen met een beperkt risico.

70. Vereisten voor gebruikersverantwoordelijken (art. 4 en 50(3-4) AI Act).

Transparantieverplichtingen

- Blootgestelde personen informeren over toegestane systemen van emotieherkenning of biometrische categorisering (informeren over emotionele herkenning).
- Bekendmaken als beeld-, audio- of videocontent is gegenereerd of bewerkt door een AI-systeem (label: deepfakes).

- De verplichting van AI-geletterdheid wordt tevens omschreven in hoofdstuk 1, art 4. AI-geletterdheid (m.i.v. 2-2-2025):
  'Aanbieders en gebruikers van AI-systemen dienen maatregelen te nemen om, naar beste vermogen, een voldoende niveau van AI-geletterdheid te waarborgen bij hun personeel en andere personen die betrokken zijn bij de exploitatie en het gebruik van AI-systemen namens hen. Hierbij moet rekening worden gehouden met hun technische kennis, ervaring, opleiding en training, de context waarin de AI-systemen worden ingezet, en de personen of groepen personen waarop de AI-systemen van toepassing zijn.'
  Het is voor organisaties van cruciaal belang om nu al wel maatregelen te nemen om ervoor te zorgen dat iedereen voldoende kennis heeft om met AI-systemen te werken. Hoewel het vereiste niveau van AI-geletterdheid kan variëren afhankelijk van specifieke taken en toepassingen, moeten alle medewerkers die met AI-systemen werken beschikken over enkele kerncompetenties. De belangrijkste hiervan zijn:
  e. AI herkennen: Het vermogen om AI-toepassingen te herkennen en inzicht te krijgen in hoe deze in het dagelijks leven worden gebruikt
  f. AI begrijpen: Begrip van de basisconcepten van AI, zoals machine learning en taalmodellen, en het onderscheiden van verschillende soorten AI en hun toepassingen.
  g. Praktisch gebruik: Vaardigheden om AI-tools effectief toe te passen in diverse contexten.
  h. Kritische evaluatie: Bewustzijn van de ethische vraagstukken en de maatschappelijke impact van AI.
  Handreiking AP: https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid

X: Ja, wij zijn gebruikersverantwoordelijke van systemen met een beperkt risico en voldoen aan het bovenstaande.

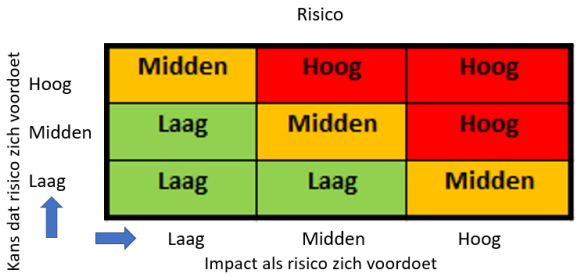
Aanvulling:
De verplichtingen inzake emotieherkenning, biometrische categorisering en deepfakes zijn niet van toepassing op deze AI-toepassing. De AI-tool analyseert uitsluitend tekstuele dossierinformatie en genereert geen synthetische audio-, beeld- of videocontent.
Ten aanzien van AI-geletterdheid zijn reeds maatregelen getroffen, waaronder een AI-beleid, menselijke beoordeling van AI-output, bewustwording van AI-risico's en periodieke bewustwordingssessies.

O: Ja, wij zijn gebruikersverantwoordelijke van systemen met een beperkt risico en voldoen niet aan het bovenstaande.
O: Nee, wij zijn geen gebruikersverantwoordelijke van systemen met een beperkt risico.

6. Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking

71. Rechtmatigheid Beoordeel, aanvullend op wat hierboven al is uitgewerkt, de rechtmatigheid van de verwerking.
'Rechtmatigheid' is een van de 6 basisprincipes (beginselen) van de AVG. Om rechtmatig te zijn, moet een verwerking in elk geval zijn gebaseerd op een grondslag uit de AVG. Maar ook mag de verwerking niet in strijd zijn met andere wetgeving, zoals een wettelijke geheimhoudingsplicht. De verwerking is rechtmatig. De verwerking: • dient een gerechtvaardigd doel; • is noodzakelijk; • voldoet aan artikel 6 AVG; • voldoet aan artikel 9 AVG; • is contractueel afgedekt.
72. Noodzaak Zijn alle verwerkingen noodzakelijk voor het bereiken van het doel?
De verwerking is noodzakelijk. Handmatige beoordeling van grote medische dossiers leidt tot: • hogere werkdruk; • langere doorlooptijden; • grotere kans op inconsistenties.
73. Dataminimalisatie en doelbinding (zie bijlage 3) Zijn alle persoonsgegevens strikt noodzakelijk voor het bereiken van het doel? En wordt aan de eis van doelbinding voldaan?
De gegevens worden alleen gebruikt voor de hierboven gespecificeerde doeleinden en niet voor andere doeleinden zonder aanvullende toestemming van de betrokkenen. Voorafgaande pseudonimisering wordt toegepast. Direct identificerende gegevens worden verwijderd.
74. Proportionaliteit Staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoelen?
De voordelen voor: • kwaliteit • snelheid • consistentie wegen op tegen de beperkte privacy-inbreuk.
75. Subsidiariteit Is er geen andere, voor betrokkene minder belastende manier om hetzelfde doel te bereiken?
Alternatieven zijn onderzocht. Er zijn geen minder ingrijpende alternatieven beschikbaar die hetzelfde niveau van ondersteuning, consistentie en efficiëntie bieden bij de analyse van medische dossiers.

7. Risicobeoordeling voor betrokkenen



De netto-risico's voor betrokkenen Het netto-risico betreft het risico voor betrokkenen inclusief de aanbevolen/aanvullende maatregelen		**(H) Hoog** **(M) Midden** **(L) Laag**
1	Discriminatie/reputatieschade van een individu (bijv. geen kans op promotie) met als gevolg aanzienlijk economisch of maatschappelijk nadeel. (overweging: medische gegevens worden verwerkt; AI-output onjuist kan zijn; een onjuiste analyse gevolgen kan hebben voor een bezwaarprocedure of medische beoordeling)	K= Laag, I = Hoog **M**
2	Identiteitsdiefstal of -fraude met als gevolg financiële verliezen (overweging: mogelijk BSN; geen IBAN; pseudonimisering; beperkte financiële fraudegevoeligheid)	K= Laag, I = Laag **L**
3	Verlies van vertrouwelijkheid van door beroepsgeheim beschermde gegevens (bijvoorbeeld bij de beroepsuitoefening van een arts) (overweging: gezondheidsgegevens; medische dossiers; rapportages van artsen; gegevens die onder (afgeleid) medisch beroepsgeheim vallen; beveiligingsmaatregelen getroffen)	K= Laag, I = Hoog **M**
4	Beperking van uitoefening van rechten of vrijheden individu (overweging: AVG-procedures, menselijke beoordeling)	K= Midden, I = Laag **L**
5	Verhindering uitoefening controle over diens persoonsgegevens (overweging: zie hierboven; de betrokkenen behouden hun AVG-rechten)	K= Laag, I = Laag **L**
6	Evalueren van persoonlijke aspecten (*profilering*) (overweging: geen profilering; geen scoring; geen classificatie; geen geautomatiseerde besluitvorming)	K= Laag, I = Laag **L**
7	Verwerking van persoonsgegevens van kwetsbare personen (overweging: er worden mogelijk gegevens van minderjarigen, zwangere vrouwen, werknemers met psychische aandoeningen en zieke werknemers verwerkt)	K= Laag, I = Hoog **M**
8	Onjuiste AI-output (hallucinaties)	K= Laag, I = Hoog **M**

	(overweging: menselijke beoordeling; BIG-geregistreerde eindverantwoordelijkheid; kwaliteitscontroles.)	
9	Automation Bias (gebruikers vertrouwen te veel op AI-output en controleren deze onvoldoende) (overweging: menselijke beoordeling verplicht; AI-geletterdheid; steekproeven)	K= Laag, I = Hoog **M**
10	Onvoldoende pseudonimisering (overweging: pseudonimisatieprotocol; gescheiden sleutelbeheer; periodieke validatie)	K= Laag, I = Hoog **M**
11	Onvoldoende verwijdering van gegevens (overweging: verwijderprocedure; verwijderrapportage)	K= Laag, I = Hoog **M**
12	Onvoldoende transparantie richting betrokkenen (overweging: privacyverklaring; cliëntinformatiebrief)	K= Laag, I = Midden **L**
13	Leveranciersafhankelijkheid (vendor lock-in) (overweging: exit-strategie; contractuele afspraken.)	K= Laag, I = Midden **L**
14	Onvoldoende monitoring van modelwijzigingen (overweging: evaluaties; incidentmanagement)	K= Laag, I = Midden **L**
15	Toegang vanuit derde landen (overweging: contractuele afspraken; logging; leveranciersbeoordeling) NB: Kans kan naar 'laag' indien expliciet is aangetoond.	K= Midden, I = Midden **M**
16	Onvoldoende AI-geletterdheid (overweging: AI-beleid; trainingen)	K= Laag, I = Hoog **M**
17	Uitval van AI-dienst (overweging: handmatig fallback-proces)	K= Laag, I = Laag **L**

8. Is voorafgaande raadpleging AP nodig?

Bepaal en omschrijf aan de hand van de resterende risico's of de verwerking mag worden gestart of dat een voorafgaande raadpleging bij de AP nodig is.
Uit deze DPIA is niet naar voren gekomen dat de beoogde verwerking een hoog restrisico oplevert voor betrokkenen. (Voorafgaande) raadpleging bij de Autoriteit Persoonsgegevens is daarom niet nodig.

9. Monitoring en evaluatie

Wijzigingen in welke vorm dan ook (economische veranderingen, nieuwe trends, wet- en regelgeving) kunnen impact hebben op de risico's, genoemd in deze DPIA. Daarom is een periodieke evaluatie (minimaal eens per jaar) aan te bevelen en maakt onderdeel uit van de PDCA-cyclus.

Periodieke evaluatie kan bestaan uit:

- Evaluatie van de effectiviteit van de genomen maatregelen en aanpassing indien nodig.
- Evaluatie Incidentanalyse en lessons learned na eventuele datalekken of fouten.
- Evaluatie AI-tool om ervoor te zorgen dat deze blijft voldoen aan de wet- en regelgeving.
- Regelmatige herziening van de DPIA om ervoor te zorgen dat deze up-to-date blijft met betrekking tot nieuwe risico's of wijzigingen.

10. Ondertekening

Betreft	**Door (naam, functie, datum)**
De DPIA is ingevuld door	Christel Bastiaenssens
De DPIA blijft onder review en beheer van	Prospectief, Shajan Omar
Goedkeuring DPIA door directie	Prospectief, Ulla Al-Saad

Uiterste datum update DPIA: **juli 2027**

Bijlagen

Bijlage 1 Privacy principes

1. Doelbinding
Persoonlijke gegevens morgen slechts worden verzameld voor legitieme doeleinden en alleen als je die expliciet hebt aangegeven en daar toestemming voor hebt gevraagd en gekregen. Je mag die gegevens verder niet gebruiken voor doelen die hiermee niet in overeenstemming zijn. Als je een theater bent is het waarschijnlijk toegestaan om aan bestaande klanten een cd van een theatershow aan te bieden die ze bezocht hebben. Maar tenzij klanten daar expliciet toestemming voor hebben gegeven, is het niet toegestaan om een theaterreis naar Rome aan te bieden.

2. Dataminimalisatie
Persoonlijke gegevens dienen adequaat en relevant te zijn voor de doelen die je hebt aangegeven. Je mag niet meer gegevens verzamelen dan nodig voor de aangegeven doelen en ook niet langer bewaren dan nodig. Bijvoorbeeld het vragen naar de kleur ogen kan relevant zijn voor een schoonheidssalon, maar is waarschijnlijk niet relevant voor een fondsenwerver. Dataminimalisatie houdt bijvoorbeeld ook in dat als een individu zich uitschrijft van jouw dienstverlening, je alleen die gegevens van hem bewaart die wettelijk verplicht zijn of noodzakelijk om later aan je administratieve verplichtingen te voldoen.

3. Accuraatheid
Je moet redelijke stappen ondernemen om de persoonlijke gegevens up-to-date te houden en bij te werken indien ze niet meer accuraat zijn. Wat redelijk is en hoe actief je daarin moet zijn, is afhankelijk van het soort relatie en het soort gegevens waarom het gaat. Als je een ziekenhuis bent, zul je vaker moeten checken of de gegevens nog correct zijn dan wanneer je online kattenvoer verkoopt. Als een klant zijn contactgegevens bijwerkt moet je die nieuwe gegevens gebruiken en mag je geen contact meer opnemen op basis van de oude gegevens.

4. Niet langer bewaren dan nodig
Je mag persoonlijke gegevens niet langer bewaren dan nodig is om aan de doeleinden te voldoen waarvoor je toestemming hebt verkregen. Gegevens die verouderd zijn of niet meer nodig moeten adequaat verwijderd worden. Als een nieuwsbriefinschrijver bijvoorbeeld aangeeft dat hij geen marketinginformatie meer wil ontvangen, dan dien je net genoeg informatie te bewaren om te zorgen dat je hem uit je marketingactiviteiten kunt verwijderen. Als een recente klant met een openstaande bestelling hetzelfde vraagt, dan mag je ook de informatie bewaren die nodig is om zijn order te kunnen verwerken.

5. Inzage-, correctie- en verwijderrecht en dataportabiliteit
Individuen hebben het recht om hun persoonlijke gegevens in te zien, te laten corrigeren en om reeds verstrekte toestemming voor bepaalde toepassingen zoals het gebruik voor direct marketing in te trekken. Ook hebben ze het recht om schadevergoeding te vragen als hun gegevens op straat komen te liggen. In sommige gevallen hebben ze ook het recht om te vragen dat hun gegevens worden verwijderd of vernietigd: het recht om vergeten te worden. Je moet de gegevens dan ook fysiek wissen of anonimiseren dus alleen een record op do-not-mail zetten is niet toereikend. Overigens mogen individuen alleen gegevens opvragen die op hen betrekking hebben – dat mag ook

per e-mail, fax of per post – en je dient dan ook te controleren of degene die de informatie opvraagt daadwerkelijk het recht heeft om deze in te zien. Een nieuw recht is ook dat van dataportabiliteit, wat inhoudt dat klanten kunnen verzoeken dat zij hun persoonsgegevens in een standaardformaat van jou ontvangen, zodat zij hun gegevens makkelijk kunnen doorgeven aan een andere leverancier. Of zelfs dat jij al hun persoonsgegevens zonder kosten naar een andere leverancier overzet, bijvoorbeeld van de ene bank naar de andere.

6. Beveiliging

Je bent verplicht om organisatorische, fysieke en technische maatregelen te treffen om persoonlijke data te beveiligen op een niveau dat overeenstemt met de gevoeligheid van die data. Dus als je een bank bent dan zul je een zwaarder beveiligingssysteem moeten hebben dan een boekwinkel, omdat de mogelijke gevolgen van een inbreuk op de persoonsgegevens groter zijn. Je mag gegevens ook niet verplaatsen naar andere landen die niet hetzelfde niveau van databescherming hebben zonder expliciete toestemming van je klanten. Je moet kunnen aantonen dat je adequate beveiligingsmaatregelen hebt getroffen. Ook als je externe dienstverleners gebruikt – de zogenaamde verwerkers – blijf je verantwoordelijk voor wat er met de gegevens gebeurt.

7. Verantwoordelijkheid

In geval van een datalek ben je verplicht om dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Brengt het lek risico's met zich mee voor de rechten en vrijheid van individuen, dan dien je ook de betrokken direct op de hoogte te stellen.

Verder moet je data protection impact assessments uitvoeren om de impact van projecten op privacy te voorspellen en om aanpassingen door te voeren waar nodig.

Veel organisaties zijn tevens verplicht om een gegevensbeschermingsfunctionaris (data protection officer ofwel DPO) te benoemen die verantwoordelijk is voor alles met betrekking tot de veiligheid van persoonlijke gegevens. In ieder geval moet je er een benoemen als:

- Je een overheidsinstantie of overheidsorgaan bent;
- Je regelmatig of stelselmatig personen monitort middels dataverwerking. Hieronder valt ook elke vorm van tracking en profilering op internet of offline, dus ook behavioural advertising, en e-mail retargeting;
- Als je gevoelige persoonlijke gegevens verwerkt, zoals ras of etnische afkomst, politieke opvattingen, seksuele gerichtheid, religieuze of levensbeschouwelijke overtuigingen, medische gegevens, strafrechtelijke gegevens of het lidmaatschap van een vakbond. Voor het mogen verwerken van gevoelige gegevens gelden overigens sowieso bijzondere aanvullende regels.

Bijlage 2 Grondslagen

1. Toestemming

De eerste grondslag die de AVG in artikel 6 noemt is de toestemming. Toestemming kan gegeven worden door een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting. De toestemming moet uitdrukkelijk zijn. Stilzwijgende toestemming is niet voldoende. Bovendien mag toestemming ook weer worden ingetrokken en moet dat net zo gemakkelijk zijn als het geven van de toestemming. Als dat gebeurt ben je dus je grondslag kwijt en mogen de persoonsgegevens niet meer verwerkt worden. Deze grondslag is vooral een vangnet, een soort restbepaling, voor het geval je van geen van de andere grondslagen gebruik kunt maken.

2. Uitvoering van de overeenkomst

De tweede grondslag maakt verwerking van persoonsgegevens mogelijk wanneer dat nodig is voor de uitvoering van de overeenkomst. Het gaat dan uiteraard om een overeenkomst waarbij de betrokkene (de persoon waarvan de persoonsgegevens zijn) partij is. Belangrijk is dat de overeenkomst niet uitgevoerd kan worden zonder die persoonsgegevens. Denk bijvoorbeeld aan een webwinkel die een naam en adres nodig heeft om producten te kunnen leveren. Is het verwerken van de persoonsgegevens alleen maar handig, maar niet noodzakelijk, dan kan deze grondslag niet gebruikt worden.

3. Wettelijke verplichting

Soms bestaat er een wettelijke verplichting op basis waarvan je persoonsgegevens wel moet verwerken. Die verplichtingen staan dan in een andere wet. Denk bijvoorbeeld aan facturen die 7 jaar bewaard moeten worden. Je bent niet verplicht om daar een contactpersoon in op te nemen, maar gegevens van eenmanszaken zijn ook persoonsgegevens. Je moet dan toch die factuur, juist inclusief die gegevens van de eenmanszaak, bewaren. Ook loonadministratie moet 7 jaar bewaard worden. Daaronder vallen ook de arbeidsovereenkomsten, ziektestaten en een kopie identiteitsbewijs.

4. Vitale belangen

Om de vitale belangen van een natuurlijk persoon te kunnen beschermen, mogen de persoonsgegevens verwerkt worden. Maar alleen als de verwerking noodzakelijk is om die vitale belangen te kunnen beschermen. Er is niet zo snel sprake van een vitaal belang. Vitaal wil zeggen dat het gaat om het leven van de persoon. Niet zozeer de algemene medische gegevens, maar wel in het geval van een ongeval, bijvoorbeeld, waarbij persoonsgegevens verwerkt worden om iemand op dat moment te kunnen behandelen. Van deze grondslag kan, maar ook mag bijna nooit gebruik gemaakt worden. Deze grondslag mag alleen worden gebruikt als een andere grondslag niet mogelijk is en er toch een noodzaak bestaat om de gegevens te verwerken om het vitale belang te beschermen (kwestie van leven of dood).

5. Algemeen belang

Als er een taak van algemeen belang vervuld moet worden waarvoor de verwerking van persoonsgegevens noodzakelijk is, dan mogen de persoonsgegevens verwerkt worden. Dit geldt ook voor taken in het kader van de uitoefening van het openbaar gezag die aan de verwerkersverantwoordelijke zijn opgedragen. Hieronder vallen onder meer de gebruikelijke verwerkingen van, voor of namens de overheid. Voor deze grondslag zal meestal ook een andere wettelijke grondslag moeten bestaan. Bijvoorbeeld omdat in een wet een bepaalde taak of

verplichting is opgenomen. Een van de rechten van de betrokken, uit de AVG, is het recht op gegevenswissing. Ook wel bekend als het recht op vergetelheid. Als persoonsgegevens echter op de grondslag algemeen belang worden verwerkt, dan bestaat het recht op gegevenswissing niet. Misschien ook niet zo gek, want anders zouden gemeenten de BRP (Basisregistratie Personen, waaronder het voormalige GBA valt) niet bij kunnen houden (gemeenten/journalistiek).

6. Gerechtvaardigd belang

Het gerechtvaardigd belang is eigenlijk vooral een belangenafweging. De verwerking moet noodzakelijk zijn voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, tenzij de privacybelangen van de betrokkene zwaarder wegen. Hierbij moet bijvoorbeeld rekening gehouden worden met de vraag in hoeverre de betrokkene had mogen verwachten dat de verwerking plaats zou vinden en met welk doel dan. Dit belang kan bijvoorbeeld gebruikt worden om direct marketing mogelijk te maken. Let wel op dat een betrokkene altijd bezwaar mag maken tegen direct marketing en de verwerking dan moet stoppen. Het gerechtvaardigd belang is ook belangrijk voor fotografen die bijvoorbeeld fotograferen op evenementen, journalistieke of documentaire fotografie verzorgen waarbij een quitclaim niet mogelijk is of wanneer het gaat om straatfotografie.

Bijlage 3 Doelbinding

Naast een geldige grondslag, is er ook nog een gerechtvaardigd doel nodig (artikel 6 lid 4 AVG). Gegevens mogen op basis van een grondslag verwerkt worden, maar dat mag alleen voor een bepaald doel. Die doelen staan niet in de AVG genoemd, maar moeten dus wel gerechtvaardigd zijn. De verwerking van de persoonsgegevens mag alleen plaatsvinden voor dat doel. Ook die doelen moeten in de privacyverklaring worden opgenomen. Zo kun je bijvoorbeeld op basis van het gerechtvaardigd belang persoonsgegevens verwerken voor direct marketingdoeleinden.

Soms kan een grondslag ook samenvallen met een doel. Zo kun je op basis van de grondslag wettelijke verplichting persoonsgegevens verzamelen met als doel te voldoen aan de administratieve bewaarplicht.

Bijlage 4 Rechten van betrokkene

1. Het recht op inzage
Het recht op inzage is het recht van betrokkenen om de persoonsgegevens die van hen verwerkt worden, in te zien.

2. Het recht op vergetelheid
Het recht op vergetelheid is het recht om 'vergeten' te worden. De organisatie moet dan persoonsgegevens wissen op verzoek van de betrokkene. Er zijn situaties denkbaar waarin dit recht niet geldt, bijvoorbeeld als de organisatie de gegevens verwerkt omdat er een wettelijke verplichting is.

3. Het recht op rectificatie
Mensen hebben het recht om persoonsgegevens die een organisatie van hen verwerkt te wijzigen en aan te vullen, zodat deze correct worden verwerkt.

4. Het recht op dataportabiliteit
Dit betekent het recht om persoonsgegevens over te dragen aan een andere organisatie.

5. Het recht op beperking van de verwerking
Het recht op beperking van de verwerking geeft de betrokkene het recht om minder gegevens te laten verwerken.

6. Het recht op een menselijke blik bij geautomatiseerde besluitvorming/profiling
De AVG geeft mensen recht op een menselijke blik bij besluiten die over hen gaan. Sommige organisaties nemen namelijk besluiten op basis van automatisch verwerkte gegevens. Bijvoorbeeld bij de automatische weigering van een online ingediende kredietaanvraag of bij verwerking van sollicitaties via internet zonder menselijke tussenkomst.

7. Het recht van bezwaar
Mensen hebben het recht om bezwaar te maken tegen het verwerken van hun persoonsgegevens. Dit recht is van bezwaar is van toepassing als een organisatie persoonsgegevens gebruikt voor marketing doeleinden. Ook kan iemand om bijzondere persoonlijke redenen gebruik willen maken van dit recht.

8. Het recht op informatie
Een betrokkene heeft recht op heldere informatie over het verzamelen en verwerken van persoonsgegevens. Bijvoorbeeld: welke persoonsgegevens verwerkt de organisatie en waarom? Organisaties geven deze informatie meestal via een privacyreglement op hun website.

Bijlage 5 Algoritme

Een AI-systeem heeft altijd een algoritme. Een algoritme is een reeks stappen of instructies die een computer volgt om een bepaald probleem op te lossen of een taak uit te voeren. In het geval van AI-systemen zijn deze algoritmen vaak complex en ontworpen om specifieke doelen te bereiken, zoals patroonherkenning, voorspelling, of beslissingsondersteuning.

Bijvoorbeeld:

- **Machine learning**-algoritmen gebruiken data om modellen te trainen die voorspellingen kunnen doen of patronen kunnen herkennen.
- **Neurale netwerken**, die worden gebruikt in deep learning, volgen een algoritmische structuur waarbij gegevens door meerdere lagen van "neuronen" worden geleid om complexe relaties in de data te leren.
- **Optimalisatie-algoritmen** worden gebruikt om de beste oplossing voor een gegeven probleem te vinden, zoals het trainen van een model om de nauwkeurigheid te maximaliseren.

Zonder een algoritme zou een AI-systeem niet kunnen functioneren, omdat het algoritme de fundamentele logica biedt waarmee de AI werkt.

Dus:

- Een AI-systeem heeft altijd een algoritme.
- Een algoritme hoeft niet altijd AI te zijn!

Bijlage 6 Algoritmeregister van de Nederlandse overheid

Het Algoritmeregister is een openbaar register waarin organisaties die vallen onder de Nederlandse overheid informatie beschikbaar stellen over de algoritmen die zij gebruiken. Dit register is bedoeld om transparantie te bieden over de werking van algoritmen, met name wanneer deze invloed hebben op de rechten en vrijheden van individuen. Het Algoritmeregister maakt het voor burgers en toezichthouders mogelijk om inzicht te krijgen in hoe en waarom bepaalde algoritmen worden gebruikt, welke gegevens worden verwerkt, en welke mogelijke gevolgen dit heeft.

Over algoritmes (overheid.nl)

Het algoritmeregister van de Nederlandse overheid

Doelen van het Algoritmeregister

1. **Transparantie**: Het register bevordert transparantie over het gebruik van algoritmen, vooral in situaties waarin algoritmen beslissingen nemen die invloed hebben op individuen.
2. **Verantwoording**: Het helpt organisaties om verantwoording af te leggen over hun gebruik van algoritmen en de manier waarop deze worden ontwikkeld en toegepast.
3. **Bewustzijn**: Het vergroot het bewustzijn bij burgers over de algoritmen die hun leven kunnen beïnvloeden, waardoor zij beter geïnformeerd zijn over hun rechten en de impact van technologie.

Inhoud van het Algoritmeregister

In het Algoritmeregister kunnen de volgende elementen worden opgenomen:

- **Beschrijving van het algoritme**: Welke taken het algoritme uitvoert en in welke context het wordt gebruikt.
- **Doel en toepassingsgebied**: Wat het doel is van het gebruik van het algoritme en in welke situaties het wordt toegepast.
- **Gegevens die worden verwerkt**: Informatie over de soorten gegevens die het algoritme gebruikt en verwerkt.
- **Invloed op burgers**: Een uitleg van hoe het algoritme beslissingen neemt en welke invloed dit kan hebben op individuen.
- **Maatregelen voor gegevensbescherming**: Informatie over hoe de privacy en gegevens van individuen worden beschermd.
- **Bias en ethische overwegingen**: Eventuele maatregelen die worden genomen om bias te voorkomen en ethische kwesties aan te pakken.
- **Contactinformatie**: Gegevens van de verantwoordelijke organisatie, zodat burgers vragen kunnen stellen of klachten kunnen indienen.

Toepassing van het Algoritmeregister

Het Algoritmeregister is in opkomst in verschillende landen, vooral binnen de publieke sector. Overheden, gemeenten, en publieke instanties worden steeds vaker verplicht of aangemoedigd om hun gebruik van algoritmen te registreren in een dergelijk register. Dit maakt deel uit van bredere initiatieven om het gebruik van kunstmatige intelligentie en geautomatiseerde besluitvorming transparanter en verantwoorder te maken.

Waarom is het belangrijk?
Met de toenemende invloed van AI en geautomatiseerde systemen op het dagelijks leven, is het Algoritmeregister een cruciaal instrument om ervoor te zorgen dat deze technologieën op een eerlijke, transparante en verantwoorde manier worden gebruikt. Het draagt bij aan het vertrouwen van het publiek in technologie en biedt hen de middelen om geïnformeerde keuzes te maken en hun rechten te beschermen.

Conclusie
Het Algoritmeregister is een belangrijk middel om transparantie en verantwoording te bevorderen in het gebruik van algoritmen die gebruikt worden door de Nederlandse overheid, vooral in situaties waarin deze een significante impact hebben op de rechten en vrijheden van individuen. Het helpt om inzicht te geven in de werking van algoritmen en zorgt ervoor dat organisaties zich bewust zijn van hun verantwoordelijkheden bij het inzetten van deze technologieën.

Bijlage 7 Bias

Bias, in de context van AI en machine learning, verwijst naar een systematische vertekening of vooroordeel in de gegevens, algoritmes, of modellen die leiden tot oneerlijke of onnauwkeurige resultaten. Bias kan verschillende vormen aannemen, afhankelijk van waar het in het proces optreedt en hoe het de uitkomsten beïnvloedt. Hier zijn enkele belangrijke soorten bias:

1. Data Bias
Voorbeeld: Als de gegevens die worden gebruikt om een AI-model te trainen niet representatief zijn voor de volledige populatie, kan het model verkeerde aannames maken. Bijvoorbeeld, als een AI voor gezichtsherkenning voornamelijk is getraind op foto's van mensen met een lichte huidskleur, kan het minder nauwkeurig zijn in het herkennen van mensen met een donkere huidskleur.

2. Algorithmic Bias
Voorbeeld: Bias kan ook worden geïntroduceerd door de manier waarop een algoritme is ontworpen. Bijvoorbeeld, een AI die sollicitaties beoordeelt en is geprogrammeerd om voorkeur te geven aan bepaalde termen of patronen, kan onbedoeld vrouwen of minderheden benadelen als het algoritme is getraind op historische gegevens waarin bepaalde groepen ondervertegenwoordigd zijn.

3. Confirmation Bias
Voorbeeld: Dit treedt op wanneer het model of de gebruiker alleen gegevens gebruikt of zoekt die hun bestaande aannames of hypotheses bevestigen, waardoor andere relevante informatie over het hoofd wordt gezien.

4. Selection Bias
Voorbeeld: Dit gebeurt wanneer de gegevens die worden gebruikt voor het trainen van een model niet willekeurig of representatief zijn gekozen, wat kan leiden tot vertekende resultaten. Bijvoorbeeld, een medisch AI-model dat alleen is getraind op gegevens van patiënten uit een bepaalde regio kan minder nauwkeurig zijn voor patiënten uit andere regio's.

5. Measurement Bias
Voorbeeld: Dit gebeurt wanneer de manier waarop gegevens worden verzameld en gemeten systematisch is vertekend. Als een AI-model bijvoorbeeld afhankelijk is van zelfgerapporteerde gezondheidsgegevens, kunnen er vertekeningen optreden als bepaalde groepen mensen systematisch verschillende antwoorden geven.

<u>Gevolgen van Bias in AI</u>

Bias in AI kan leiden tot onrechtvaardige of discriminerende uitkomsten, zoals:

- Ongelijke behandeling: Een AI-systeem dat bias bevat, kan bepaalde groepen mensen benadelen, bijvoorbeeld door hen lagere scores te geven in kredietbeoordelingen of hen minder kans te geven op een baan.
- Verminderde nauwkeurigheid: Als de AI verkeerde aannames maakt door bias, kan dit leiden tot onnauwkeurige voorspellingen of beslissingen.

- Verlies van vertrouwen: Wanneer mensen ontdekken dat een AI-systeem biased is, kan dit leiden tot een verlies van vertrouwen in de technologie.

Oplossingen voor Bias

Om bias te verminderen, kunnen ontwikkelaars:

- Zorgvuldig en representatief trainingsdata verzamelen.
- Bias-detectie en -correctie methoden implementeren.
- Transparantie bevorderen, zodat gebruikers begrijpen hoe beslissingen worden genomen.
- Menselijke controle inbouwen om AI-uitkomsten te beoordelen en bij te stellen.

Bias is een belangrijk aandachtspunt in de ontwikkeling en implementatie van AI-systemen, omdat het directe gevolgen kan hebben voor de eerlijkheid en effectiviteit van de technologie.

Bijlage 8 Definities

Algoritme
Een algoritme is een reeks stappen of instructies die een computer volgt om een bepaald probleem op te lossen of een taak uit te voeren. In het geval van AI-systemen zijn deze algoritmen vaak complex en ontworpen om specifieke doelen te bereiken, zoals patroonherkenning, voorspelling, of beslissingsondersteuning.

Artificial Intelligence (AI)
Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan *aanpassingsvermogen* kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.

Betrokkene (of datasubject)
Een betrokkene of datasubject is een natuurlijk persoon van wie u als organisatie persoonsgegevens verwerkt. Voorbeelden van een betrokkene kunnen een individu, client/patiënt, een klant, een potentiële klant, een werknemer, een contactpersoon, etc. zijn.

Bias
Bias, in de context van AI en machine learning, verwijst naar een systematische vertekening of vooroordeel in de gegevens, algoritmes, of modellen die leiden tot oneerlijke of onnauwkeurige resultaten. Bias kan verschillende vormen aannemen, afhankelijk van waar het in het proces optreedt en hoe het de uitkomsten beïnvloedt.

Bijzondere persoonsgegevens
De AVG refereert aan gevoelige persoonsgegevens als “speciale categorieën van persoonsgegevens.” De speciale categorieën van persoonsgegevens omvatten ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijk opvattingen, lidmaatschap van een vakbond, seksuele gerichtheid, en gezondheid, genetische en biometrische gegevens waar verwerkt tot een uniek te identificeren individu. Persoonsgegevens gerelateerd tot criminele veroordelingen en overtredingen zijn niet inbegrepen, maar verglijkbare waarborgen zijn hier van toepassing.

Derde
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris Gegevensbescherming (FG)
De benoeming van een Functionaris voor de Gegevensbescherming is verplicht indien verwerkingen wordt uitgevoerd door een publieke autoriteit of wanneer de “kernactiviteiten” van een verwerkings-verantwoordelijke “reguliere en systematische monitoring van datasubjects op een grote schaal betreffen,” of bestaat uit het verwerken van speciale categorieën van gegevens of gegevens over criminele veroordelingen “op een grote schaal”.

Gegevensbeschermingseffectbeoordeling (DPIA)
De AVG beschikt over een nieuwe verplichting rond de verwerkingsverantwoordelijken en gegevensverwerker een gegevensbeschermingseffectbeoordeling uit te voeren (ook bekend als een

Data Protection Impact Assessment, of Privacy Impact Assessment (PIA)) alvorens het uitvoeren van enige verwerking dat een specifiek gegevensrisico toont door z'n aard, toepassingsgebied, of doelen.

Gegevens over gezondheid
Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Inbreuk in verband met persoonsgegevens
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Ontvanger
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk 4.5.2016 L 119/33 Publicatieblad van de Europese Unie NL persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Pseudonimisering
Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming (van de betrokkene)
Elke “vrijelijk gegeven, specifieke, geïnformeerde en ondubbelzinnige” indicatie van de wensen van het individu bij welke het datasubject, of door een verklaring of door een heldere actieve handeling, te kennen geeft in te stemmen met de persoonsgegevens verbonden aan hen om te worden verwerkt voor een of meerder doelen.

De actieve handeling, of een positieve opt-in, betekent dat de toestemming niet kan worden afgeleid van stilte, voor aangekruiste hokjes, of inactiviteit. Het dient eveneens afgescheiden te zijn van de voorwaarden, en een eenvoudige wijze van herroepen hebben. Publieke autoriteiten en werknemers zullen bijzondere aandacht moeten schenken aan het feit dat de toestemming vrijelijk is gegeven.

De bestaande toestemming hoeft niet automatisch te worden vernieuwd in de voorbereiding op de AVG, maar ze dienen aan de AVG-norm te voldoen als het gaat om specifiek zijnde, granulair, helder, opt-in, gedegen gedocumenteerd, en makkelijk te herroepen. Indien niet, verander uw toestemmings- mechanismen en zoek een AVG GDPR-compliant toestemming, of een alternatief om toe te stemmen.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.