



GEMEENTE VELSEN

Gemeentelijke uitgangspunten voor werken met AI

Inhoudsopgave

Managementsamenvatting.....	2
Aanleiding.....	3
Doel	3
AI en Velsen	4
Scope & Afbakening.....	5
Uitgangspunten.....	6
Strategie: reguleren, faciliteren en gecontroleerd leren.....	8
Portfolio en prioritering van pilots.....	9
Kaders & Richtlijnen	11
Basisregels.....	11
Aanvullende regels GenAI.....	11
Risico's.....	12
Generatieve AI	13
Proces: Principes, LITE en DEEP scan	14
Rollen, Mandaat en Besluitvorming.....	15
Capaciteit en Middelen	15
Inkoop en leveranciers als kernonderdeel	16
Transparantie en communicatie richting inwoners	16
Privacy, informatiebeveiliging en ethiek.....	17
AI en architectuur	18
Adoptie en AI-geletterdheid: van beleid naar gedrag.....	19
Afsluiting	21
 Bijlagen	
Bijlage A: Begrippenlijst	0
Bijlage B: AI	2
Narrow AI (ANI).....	2
Artificial General Intelligence (AGI)	3
Artificial Superintelligence (ASI).....	3
Bijlage C: AI Vandaag.....	4
Generatieve AI (GenAI).....	4
Begrippen in gewone taal.....	5
Bijlage D: Algoritmes en AI in software	6
Bijlage E: Rollen AI	6
Bijlage F: Framework for Trustworthy AI	7

Managementsamenvatting

AI (Artificial Intelligence) wordt in hoog tempo onderdeel van het dagelijks werk. Binnen Velsen groeit de behoefte om AI gericht in te zetten voor betere dienstverlening, hogere kwaliteit en meer rust in werkprocessen, maar medewerkers hebben behoefte aan duidelijke kaders. Tegelijk vraagt de AI verordening (AI Act) om een risicogestuurde aanpak en aantoonbare borging. Dit document brengt die twee samen: kansen benutten én aantoonbaar in control blijven, vanuit de kernwaarden uitnodigend & transparant, doeltreffend en verantwoordelijk.

Publieke waarde is leidend. AI wordt alleen ingezet als het aantoonbaar bijdraagt aan dienstverlening, kwaliteit, toegankelijkheid of doelmatigheid. Daarom start elk initiatief met een helder doel en een beperkte set indicatoren, zodat effect en risico's gevolgd kunnen worden.

De kern is dat AI wordt benaderd als intensieve automatisering: een versneller die publieke waarde vergroot en professionals ondersteunt, met de mens als eindverantwoordelijke. De strategie bestaat uit drie sporen: reguleren met heldere richtlijnen en basisregels (met extra regels voor generatieve AI), faciliteren met een veilige, beheerde omgeving (zoals Copilot) en gecontroleerd leren via pilots die klein starten, meetbaar zijn en alleen opschalen als het verantwoord kan. Velsen kiest daarbij bewust voor Microsoft Copilot als het enige toegestane AI-platform, zodat alle data binnen de gemeentelijke omgeving blijft en niet wordt gebruikt voor modeltraining of gedeeld buiten de organisatie.

Output van GenAI wordt behandeld als concept; bij inwoner-impact en bij juridische, financiële of beleidsinhoud geldt verificatieplicht.

De organisatie werkt met drie lagen toetsing: principes en kernwaarden als “voorkeur”, een LITE-check om bij laag en beperkt risico snel en veilig te kunnen starten, en een DEEP-check voor hogere risico's of grotere impact, met expliciete onderbouwing en bewijsstukken. De risicotriage onderscheidt laag, beperkt en hoog risico, en kent daarnaast een NO-GO-categorie voor onaanvaardbaar risico. Deze aanpak staat niet los van de bestaande werkwijze, maar sluit aan op het organisatiebrede intakeproces voor aanschaf en inzet van tools, zodat er geen parallel circuit ontstaat.

Om dit werkbaar te maken zijn rolhelderheid, mandaat en expliciete capaciteit nodig voor toetsing, registratie, begeleiding en evaluatie. Dit document beschrijft wie waarvoor verantwoordelijk is, welke minimumregels altijd gelden (ook voor AI in bestaande leverancierssoftware) en hoe herbeoordeling plaatsvindt bij relevante releases, nieuwe modules of contractwijzigingen. Daarnaast wordt een vaste ritmiek ingericht voor evaluatie en bijsturing (waarde, kwaliteit, incidenten en naleving) en blijft AI-geletterdheid doorlopend onderdeel van adoptie. Hiermee ontstaat één bestuurbare lijn voor verantwoord experimenteren én gecontroleerd opschalen.

Aanleiding

Artificial Intelligence (AI) biedt kansen om publieke waarde te vergroten: betere dienstverlening, hogere kwaliteit en meer rust in werkprocessen. Medewerkers willen met AI aan de slag, maar hebben behoefte aan duidelijke kaders voor verantwoord gebruik. Tegelijk wil het DT dat AI slim, veilig en zo duurzaam mogelijk wordt benut. Zonder die kaders ontstaat versnippering, schaduwgebruik¹ en een verhoogd risico op onbedoelde datadeling. De AI-verordening vraagt bovendien om een risicogestuurde aanpak en aantoonbare borging. Voor een gemeente betekent dit dat AI niet alleen een innovatiethema is, maar ook vraagt om duidelijke sturing en naleving.

Andere gemeenten laten zien dat er vaak wel richtlijnen bestaan, maar minder vaak een samenhangende aanpak die visie, strategie, kaders, inkoop en uitvoering bij elkaar brengt. Dit document is bedoeld om die samenhang wél te bieden en om de organisatie handelingsperspectief te geven.

De vraag is niet langer of AI een plek krijgt in het werk, maar welke publieke waarde ermee wordt nagestreefd, bij welk gebruiksscenario (toepassingen) dat past, welke risico's acceptabel zijn en welke keuzes en prioriteiten daarbij horen. Dit document geeft daarop een bestuurbaar antwoord: een inspirerende aanpak, een praktische strategie en duidelijke kaders waarmee veilig geëxperimenteerd én verantwoord opgeschaald kan worden.

Deze aanpak sluit aan op de koers uit Visie op Velsen 2050: betere dienstverlening en sturing met oog voor de menselijke maat. Het past ook bij de lijn van “Smart Governance” zoals die in college uitvoeringsprogramma's wordt beschreven: dienstverlening digitaliseren waar het kan, maar tegelijk bereikbaar en aanspreekbaar blijven, met duidelijke communicatie, inzicht voor inwoners in de status van hun hulpvraag en waar mogelijk een-loket dienstverlening.

Doel

Dit document heeft drie doelen.

1. Het geeft richting aan de organisatie over wat Velsen met AI wil bereiken en onder welke voorwaarden.
2. Het beschrijft hoe de organisatie in samenhang AI stap-voor-stap invoert en professionaliseert, waar de pilots integraal onderdeel van zijn.
3. Het beschrijft welke kaders en minimumregels nodig zijn om te kunnen aantonen dat AI verantwoord wordt ingezet.

Het document is nadrukkelijk bedoeld om te publiceren en als basis te gebruiken voor besluitvorming, uitvoering en communicatie.

¹ Gebruik van IT-toepassingen die niet beschikbaar is gesteld of geautoriseerd door de organisatie.

AI en Velsen

AI is geen doel op zich. Het is intensieve automatisering, een slimme versneller die publieke waarde vergroot, routinewerk wegneemt en professionals meer tijd geeft voor beoordeling en maatwerk. Voor Velsen betekent dat betere dienstverlening voor inwoners, hogere kwaliteit en meer rust in werkprocessen, zonder dat het menselijke oordeel verdwijnt. AI is er om medewerkers te ondersteunen, niet om verantwoordelijkheid weg te automatiseren.

Die keuze vraagt om lef én discipline. Lef om te vernieuwen waar het helpt. Discipline om het goed te doen en het uit te leggen. Velsen wil AI zo inzetten dat medewerkers en inwoners zich welkom, gehoord en serieus genomen voelen. Dat betekent: helder communiceren wanneer AI wordt gebruikt, wat het doet en wat het vooral níet doet. Geen schijnzekerheid, geen “computer says no”, maar transparant werken, met ruimte voor vragen, bezwaar en herstel als er iets misgaat.

We zetten AI alleen in als het echt iets oplevert. Niet omdat het kan, maar omdat het aantoonbaar bijdraagt aan publieke waarde. Kortere doorlooptijden waar dat kan. Minder fouten en herstelwerk. Betere bereikbaarheid. Begrijpelijker communicatie. Meer tijd voor het gesprek waar de menselijke maat nodig is. Doeltreffendheid betekent bij ons niet sneller. Het betekent juister, doen wat nodig is, onderbouwd en met zichtbare impact. Daarom start elk initiatief met een concreet en afgebakend probleem, een duidelijke doelgroep en een kleine set indicatoren die je kunt volgen. Geen meetbaar effect? Dan geen opschaling.

Tegelijk blijft Velsen verantwoordelijk. AI mag adviseren, structureren en samenvatten. De regie over proces en uitkomst blijft bij mensen. Collega's moeten kunnen ingrijpen, corrigeren, pauzeren en uitleggen wat er gebeurt. Als een toepassing invloed heeft op rechten, toegang tot voorzieningen of keuzes die inwoners raken, dan gelden zwaardere eisen, zwaardere toetsing en aantoonbare borging. Dit doen we niet alleen. We betrekken de juiste expertise, escaleren als dat nodig is en we durven te stoppen als risico's of onzekerheid te groot worden.

Velsen kiest dus niet voor AI als losse innovatie, maar als een volwassen manier van werken waarin AI medewerkers ondersteunt: uitnodigend en transparant, doeltreffend in resultaten en verantwoordelijk in keuzes. Dat is de maatstaf. Niet voor een paar pilots, maar als richting voor hoe we als organisatie met technologie omgaan. Vandaag, en straks als systemen slimmer, krachtiger en zelfstandiger worden.

Dit document geeft richting. De scope en uitgangspunten in de volgende hoofdstukken beschrijven de organisatiebrede spelregels die altijd gelden. De strategie daarna laat zien hoe Velsen dit in de praktijk organiseert.

Scope & Afbakening

Deze aanpak geldt voor alle AI-toepassingen die in Velsen worden gebruikt of ingekocht, inclusief AI die ‘verstopt’ zit in bestaande software. In de startfase ligt de nadruk op generatieve AI in het dagelijks werk, omdat daar nu de meeste vragen ontstaan en omdat medewerkers snel behoefte hebben aan houvast. Dat betekent niet dat de aanpak zich daartoe beperkt. De kaders en de toetsing (principes, LITE en waar nodig DEEP) gelden ook voor voorspellende en classificerende toepassingen én voor AI-functionnalité in bestaande en nieuw ingekochte systemen.

De aanpak maakt onderscheid tussen drie typen inzet. De eerste is generatieve AI voor tekst, samenvattingen of spraak naar tekst. De tweede is voorspellende of classificerende AI die patronen herkent en labels of signalen geeft. De derde is AI die direct invloed heeft op besluiten of toewijzing. Hoe dichter een toepassing bij besluitvorming komt, hoe zwaarder de eisen worden. Daarnaast spelen ook het type en de gevoeligheid van de gebruikte (persoons)gegevens, de schaal en de mate van autonomie een belangrijke rol in de risicobeoordeling.

Dit document is geen aankoop- of implementatieplan. Het maakt geen productkeuzes en beschrijft de technische inrichting niet tot in detail. Dat loopt via het bestaande intake- en inkoopproces en wordt, waar nodig aangevuld met de AI-checks uit deze aanpak. AI neemt geen besluiten over inwoners. Autonome besluitvorming die inwoners raakt valt buiten de scope. Toepassingen die invloed kunnen hebben op besluiten, toewijzing, rechten of toegang tot voorzieningen worden alleen ingezet als ondersteuning, met menselijk toezicht en herstelmogelijkheden. Hiervoor is expliciete toetsing via de DEEP-route verplicht. Tot slot is het gebruik van inwonersgegevens in onbeheerde of publieke AI-tools uitgesloten. Verwerking van dergelijke gegevens kan alleen in gecontroleerde oplossingen en na toetsing.

De mens blijft eindverantwoordelijk. AI mag adviseren, structureren en samenvatten, maar medewerkers houden regie over proces en uitkomst. Wanneer een toepassing invloed kan hebben op besluiten, rechten of toegang tot voorzieningen, geldt een zwaardere route. Dan is het niet genoeg dat een systeem handig is. We moeten kunnen aantonen dat het rechtmatig, veilig, uitlegbaar en herstelbaar is, met een duidelijke route voor vragen, bezwaar en correctie.

Uitgangspunten

Om AI veilig en doelgericht in te zetten, hanteert Velsen onderstaande uitgangspunten. Deze uitgangspunten gelden voor alle AI-toepassingen: zowel nieuwe pilots als AI-functionaliteit die via bestaande systemen en leverancierssoftware wordt toegevoegd. Ze sturen keuzes in intake, ontwerp, inkoop, gebruik en beheer.

Uitgangspunten

1. Publieke waarde is leidend

Velsen zet AI uitsluitend in als dit aantoonbaar bijdraagt aan publieke waarde – direct in de dienstverlening, of indirect in interne processen (zoals bedrijfsvoering, ondersteuning en uitvoering) die uiteindelijk leiden tot een betere kwaliteit, toegankelijkheid of doelmatigheid van publieke taken. Het doel en de doelgroep van AI worden altijd scherp beschreven.

2. Meetbaarheid is voorwaarde voor opschaling

Elk initiatief start met vooraf afgesproken indicator(en) en evaluatiecriteria. Zonder meetbaar effect volgt geen opschaling en geen structurele inzet.

3. Menselijk toezicht en eindverantwoordelijkheid

Alle AI-toepassingen vallen onder menselijk toezicht, waarbij de intensiteit vooraf wordt afgestemd op het risico. Wanneer AI inwoners direct raakt — zoals bij besluiten, inwonercommunicatie of juridische/financiële inhoud — geldt een strikte verificatie- en verantwoordingsplicht. Bij interne of laag-risico toepassingen volstaat proportioneel toezicht, zoals steekproeven of procescontroles.

4. Proportionaliteit: het lichtst passende middel

AI is een middel, geen doel. Als een eenvoudiger oplossing hetzelfde effect bereikt, heeft die de voorkeur.

5. Risicogestuurde aanpak: licht waar het kan, zwaar waar het moet

Velsen werkt met risicoklassen, laag, beperkt en hoog. De toetsing is proportioneel. Principes zijn de voorkeur. LITE is de snelle en veilige start. DEEP is verplicht bij hogere impact of onzekerheid.

6. Geen autonome besluitvorming die inwoners raakt

Autonome besluitvorming die inwoners raakt valt buiten scope. Toepassingen die dicht tegen besluitvorming aan liggen worden alleen ingezet na expliciete DEEP-toetsing, met menselijk toezicht en herstelmogelijkheden.

7. Geen inwonersgegevens in onbeheerde of publieke AI-tools

Gebruik van inwonersgegevens in onbeheerde/publieke AI-tools is uitgesloten. Verwerking kan alleen in gecontroleerde oplossingen en na toetsing.

8. Privacy en gegevensbescherming by design

Gegevensgebruik is minimaal en passend. Grondslag en doelen zijn vastgelegd. Waar nodig worden instrumenten ingezet zoals DPIA's, verwerkersafspraken, bewaartermijnen en verwijderafspraken. Voor GenAI betekent dit dat data-classificatie en passende handhaving onderdeel zijn van de borging.

9. Gelijke behandeling en herstel

Als AI mensen kan raken, wordt actief gekeken naar risico's op bias/uitsluiting. Er is een vastgelegde route voor vragen, bezwaar, correctie en herstel wanneer nadeel ontstaat.

10. Transparantie en uitlegbaarheid richting inwoners

Inwoners moeten kunnen herkennen wanneer AI wordt ingezet en wat dit betekent. Voor relevante toepassingen wordt begrijpelijke toelichting opgesteld en vastgelegd in het algoritmeregister.

11. Veiligheid, robuustheid en terugvalopties zijn verplicht

AI-toepassingen moeten bestand zijn tegen fouten, misbruik en onverwacht gedrag. Per toepassing worden kwaliteitsnormen en fallback/rollback vastgelegd, inclusief logging/monitoring en incidentafhandeling.

12. Leveranciers en inkoop zijn kernonderdeel van 'in control'

AI-eisen worden standaard opgenomen in inkoop en contractmanagement, inclusief transparantie over AI-functionaliteit, datagebruik, auditrechten, incidentondersteuning, release-meldplicht en een werkbare exit.

13. Eén bestuurbare lijn: aansluiten op het bestaande intakeproces

AI vormt geen parallel traject. Initiatieven lopen via de organisatiebrede intake voor informatieproducten; de AI-checks worden daaraan gekoppeld zodat besluitvorming, registratie en verantwoording op één plek landen.

14. Accountability en eigenaarschap zijn expliciet belegd

De proceseigenaar is verantwoordelijk voor waarde, scope, acceptatiecriteria en stop/door-besluitvorming. Voor pilots en live-toepassingen leggen we vooraf monitoringafspraken, evaluatiemomenten en escalatiecriteria vast. Bij overschrijding van risicogrenzen of bij onvoldoende toegevoegde waarde sturen we bij of stoppen we. Besluiten, uitzonderingen en herbeoordelingen worden vastgelegd. Velsen houdt intern een actueel overzicht bij van gebruikte AI, risicoklasse en borgingsmaatregelen.

15. AI is een beheerde toepassing: periodieke herbeoordeling is onderdeel van beheer

Niet alleen nieuwe pilots worden getoetst: ook bestaande systemen kunnen AI bevatten. Bij relevante releases, nieuwe modules of contractwijzigingen wordt opnieuw beoordeeld of AI is toegevoegd/uitgebreid en wat dit betekent voor

risico, transparantie, privacy en beveiliging. Daarnaast wordt een vaste evaluatiecyclus ingericht voor evaluatie en bijsturing.

Strategie: reguleren, faciliteren en gecontroleerd leren

De strategie heeft drie sporen die elkaar versterken.

1. Het eerste spoor is reguleren. Het gebruik van AI wordt toegestaan, met duidelijke richtlijnen voor medewerkers. In de eerste fase ligt de nadruk op generatieve AI, omdat dit nu de meest zichtbare vraag oproept. De richtlijnen gelden echter breder, ook voor voorspellende en besluit- of proces ondersteunende toepassingen. Dat voorkomt willekeur en schaduwgebruik en geeft collega's houvast in wat veilig is.
2. Het tweede spoor is faciliteren. Waar mogelijk wordt een veilige, beheerde omgeving aangeboden voor AI-toepassingen die medewerkers kunnen gebruiken in hun werk. De start ligt bij een gemeentelijke generatieve AI-voorziening die past bij gemeentelijke eisen. De gekozen voorzieningen en eisen moeten echter ook bruikbaar zijn voor andere vormen, zoals voorspellende of proces ondersteunende functionaliteit in applicaties. Deze AI-voorziening verkleint risico's rond datadeling, bewaartermijnen, onduidelijke verwerkersafspraken en onbedoelde opslag. VNG wijst erop dat gemeenten na privacytoetsen zelf moeten afwegen of risico's voldoende te mitigeren zijn of bewust worden geaccepteerd. Daarom blijven we dit volgen en actualiseren we afspraken wanneer kaders of leveranciersvoorwaarden wijzigen.

Schaalbaar verantwoord gebruik vraagt meer dan een beheerde omgeving. Daarom werkt Velsen stapsgewijs toe naar organisatiebrede data-classificatie en technische handhaving bij GenAI (toegangsrechten, labeling en waar passend Data Loss Prevention). Zo kan het gebruik van GenAI verantwoord meegroeien met de organisatie, zonder dat privacy en informatiebeveiliging onder druk komen te staan. Waar passend sluit Velsen bij de beoordeling van toepassingen aan op landelijke kaders en instrumenten, zoals het Impact Assessment Mens en Algoritmes (IAMA), als onderdeel van de LITE- en DEEP-route.

Concreet werkt Velsen nu al met de beheerde Microsoft-omgeving (Copilot) als standaardvoorziening voor generatieve AI. Die keuze is eerder gemaakt omdat organisatiebreed al met Microsoft toepassingen (licenties en beheer) wordt gewerkt en omdat deze omgeving beter aansluit op Europese kaders en afspraken rond gegevensbescherming.

Velsen hanteert daarbij een helder principe: Copilot is op dit moment het enige AI-platform dat we toestaan voor het ontwikkelen van nieuwe AI-toepassingen én voor eindgebruikers. Hiermee borgen we dat alle gegevens binnen de

gemeentelijke omgeving blijven, niet terechtkomen in publieke modellen en door Microsoft niet worden gebruikt voor het trainen van AI-systemen. Dit biedt maximale zekerheid over privacy, beveiliging en controle over onze data.

Dit uitgangspunt is niet in beton gegoten. De markt en het beleid bewegen snel. Als eisen, risico's of beschikbare oplossingen veranderen, bijvoorbeeld door nieuwe Europese of landelijke kaders of door gewijzigde leveranciersvoorwaarden, actualiseert Velsen de standaardvoorziening en de bijbehorende afspraken.

3. Het derde spoor is gecontroleerd leren door pilots. De organisatie kiest bewust voor kleinschalige initiatieven met heldere doelen, beperkte scope en vooraf afgesproken borging. Pilots worden gebruikt om kennis op te bouwen, te meten wat werkt en te bepalen wat verantwoord opgeschaald kan worden. Elk spoor werkt binnen de uitgangspunten: publieke waarde, risicogestuurd toetsen, privacy en beveiliging by design, transparantie richting inwoners en expliciet eigenaarschap. Deze uitgangspunten vormen de kern bij pilots, maar zijn geen volledige lijst: alle uitgangspunten uit dit document (zoals proportionaliteit, geen autonome besluitvorming en dataminimalisatie) zijn onverkort van toepassing op elk van de drie sporen.

Velsen kiest voor leren door te doen, maar niet vrijblijvend. Experimenteren is nodig om kennis op te bouwen en bij te blijven, maar gebeurt gecontroleerd. Pilots starten klein, met duidelijke afspraken, beperkte scope en heldere evaluatiecriteria. Wat werkt en binnen de kaders past, kan stap voor stap worden opgeschaald. Wat niet voldoet, wordt aangepast of gestopt. Zo ontstaat tempo met vertrouwen.

Deze strategie wordt niet als “los AI-programma” naast de organisatie gezet. Velsen heeft al een organisatiebreed intakeproces voor informatieproducten waarin specialisten adviseren. De bedoeling is dat principes en LITE- en DEEP-checks hierop aansluiten. In de startfase worden de checks vooral gebruikt voor pilots, zodat de werkwijze in de praktijk kan ontwikkelen. Daarna wordt de koppeling aan het reguliere intakeproces logisch en schaalbaar.

Portfolio en prioritering van pilots

Om te voorkomen dat AI-initiatieven versnipperen, worden pilots niet ad-hoc gestart maar geselecteerd en beoordeeld als één portfolio. Dat betekent dat initiatieven worden gewogen op publieke waarde, risico en haalbaarheid, en dat er bewust keuzes worden gemaakt welke pilots wel en niet tegelijk lopen. De organisatie bewaakt daarmee focus en capaciteit, zodat pilots ook echt worden afgerond, geëvalueerd en vertaald naar

beleid, richtlijnen en waar nodig opschaling. Zo ontstaat overzicht en wordt voorkomen dat er veel wordt geprobeerd, maar weinig structureel landt.

Continu inzicht en toetsing van bestaande AI-toepassingen

Naast nieuwe pilots geldt deze aanpak ook voor bestaande systemen en leverancierssoftware waarin AI-functionaliteit kan zitten, ook als die niet expliciet zo wordt genoemd. Daarom wordt structureel bijgehouden welke applicaties en processen AI bevatten en in welke risicoklasse ze vallen, met een periodieke herbeoordeling. Belangrijk is dat dit niet alleen een eenmalige inventarisatie is: bij releases, nieuwe modules of contractwijzigingen wordt opnieuw gecontroleerd of er AI is toegevoegd of uitgebreid en of dat gevolgen heeft voor risico, transparantie, privacy of beveiliging. Zo blijft de organisatie niet alleen bij nieuwe initiatieven “in control”, maar ook bij veranderingen in bestaande tooling.

Gecontroleerd leren en inventariseren werkt alleen als dit ook onderdeel wordt van het dagelijkse beheer. Functioneel applicatiebeheerders spelen hierin een sleutelrol. Van hen wordt verwacht dat zij zicht hebben op functionele en ethische implicaties van AI in ‘hun’ applicaties. Door ze te ondersteunen met kaders, checks en kennisontwikkeling groeien zij door naar een volwassen vorm van beheer waarin signaleren, beoordelen en tijdig escaleren van AI-risico's een vanzelfsprekend onderdeel is. Zo blijft de organisatie niet alleen bij nieuwe initiatieven ‘in control’, maar ook bij veranderingen in bestaande applicaties.

Inkoop en aanbesteding krijgen expliciet aandacht. Bestaande contracten worden doorgelicht op het gebruik van AI, dataverwerking en eigenaarschap van data en output. Bij nieuwe contracten en aanbestedingen worden heldere voorwaarden gesteld aan transparantie, privacy, beveiliging, auditbaarheid en naleving van wet- en regelgeving. Zo wordt voorkomen dat AI-functionaliteit ongemerkt wordt ingekocht of ingebed in leveranciersoplossingen. Dit reguleren van inkoop en contracten vormt een onderliggende randvoorwaarde die alle drie de sporen ondersteunt en versterkt.

Kaders & Richtlijnen

Om de strategie uitvoerbaar te maken, zijn duidelijke spelregels nodig. De kaders en richtlijnen geven richting in gewone taal. Ze maken ook duidelijk wanneer iets kan, wanneer verdieping nodig is en wanneer een initiatief niet past.

Velsen werkt met 7 principes² als “voordeur”, gebaseerd op Trustworthy AI. Dat is bewust: het is herkenbaar, begrijpelijk en breed genoeg voor de organisatie. De principes bieden richting, en de uitwerking gebeurt via LITE en DEEP (zie bijlage).

Deze principes zijn bedoeld om twee dingen tegelijk te doen. Ze maken ruimte om te experimenteren en ze voorkomen dat initiatieven later vastlopen op juridische of ethische problemen. Daarom zijn er naast de principes ook minimumregels en procesafspraken.

Basisregels

De basisregels concretiseren de uitgangspunten en vormen de minimale eisen die altijd gelden bij elk initiatief. Waar de uitgangspunten richting geven, maken de basisregels ze toepasbaar in de praktijk.

We starten alleen met een initiatief als:

- Het doel en de publieke waarde helder zijn én we het effect meetbaar maken;
- Er menselijk toezicht is als mensen geraakt kunnen worden;
- Het gegevensgebruik en de grondslag duidelijk en vastgelegd zijn;
- Een externe leverancier aantoonbaar voldoet aan eisen voor beveiliging, auditbaarheid en exit;
- Het middel in verhouding is: als een eenvoudiger oplossing hetzelfde effect haalt, kiezen we die.

Aanvullende regels GenAI

Voor GenAI, zoals Copilot, hanteren we aanvullende regels. Deze regels zijn bedoeld om veilig en zorgvuldig gebruik te borgen.

- Gebruik GenAI (Copilot) alleen in de beheerde omgeving; geen publieke tools voor werkcontent.
- Gebruik geen vertrouwelijke of bijzondere persoonsgegevens in prompts, tenzij expliciet goedgekeurd in een gecontroleerde oplossing.

² Bijlage 1: Framework for Trustworthy AI: Mens-centraal, Proportionaliteit, Fairness / non-discriminatie, Transparantie, Privacy & dataminimalisatie, Robuustheid & veiligheid, Accountability

- Output is concept; controleer feiten, bronnen en beleidsconsequenties, zeker bij inwoner-impact.
- Voor GenAI zijn eerder richtlijnen opgesteld. Deze richtlijnen zijn essentieel voor het gebruik van Copilot en komen neer op drie uitgangspunten:
 1. Geen persoonsgegevens invoeren in prompts: ook geen namen, adressen of BSN's van inwoners;
 2. Geen vertrouwelijke of gevoelige informatie gebruiken in Copilot Chat. Medewerkers beoordelen vooraf hoe gevoelig informatie is;
 3. Altijd kritisch blijven op de gegenereerde output: Copilot geeft conceptvoorstellen die door medewerkers inhoudelijk moeten worden beoordeeld, gecontroleerd en waar nodig gecorrigeerd.
- Norm: Velsen hanteert data-classificatie als norm voor AI-gebruik. In GenAI mogen alleen gegevens worden verwerkt die passen binnen de toegestane classificatie voor de gebruikte omgeving. Toegangsrechten, labeling en (waar beschikbaar) DLP-maatregelen borgen dat vertrouwelijke informatie niet onbedoeld wordt gedeeld of hergebruikt. Afwijkingen zijn alleen toegestaan na expliciete beoordeling in LITE/DEEP en vastlegging van maatregelen.
- Overgangsregel: Als data-classificatie en technische handhaving nog niet organisatiebreed zijn ingericht, wordt GenAI beperkt tot niet-vertrouwelijke informatie en generieke taken. Uitzonderingen zijn alleen mogelijk na expliciete beoordeling en vastlegging van maatregelen via de LITE- of DEEP-route.

Deze basisregels zorgen dat we verantwoord kunnen versnellen: met grip op privacy, veiligheid en behoorlijk bestuur, en met zo min mogelijk risico op bestuurlijke of juridische problemen.

Risico's

De AI-verordening werkt met een risicobenadering en wordt gefaseerd van toepassing. In de praktijk is daarom een eenvoudige triage nodig die bepaalt welke route een initiatief volgt. Er wordt, in overeenstemming met de AI-verordening, gewerkt met drie praktische niveaus: laag risico, beperkt risico en hoog risico.

Laag risico betreft vooral interne ondersteuning met beperkte impact, zoals samenvatten of conceptteksten, zonder gevoelige gegevens en zonder effect op rechten van inwoners. Beperkt risico betreft toepassingen met zichtbare interactie of transparantie eisen, of met meer gevoeligheid in data, schaal of toepassing. Hoog risico betreft toepassingen die mensen kunnen raken in selectie, beoordeling, toewijzing, handhaving of het sociaal domein, of die dicht tegen besluitvorming aan liggen.

Deze triage bepaalt direct welke borging nodig is. Laag en beperkt risico kunnen in principe starten via de principes en de LITE-check, mits de basisvoorwaarden op privacy, veiligheid en transparantie op orde zijn. Hoog risico volgt altijd de verdiepende route via de DEEP-check, zodat onderbouwing, bewijsstukken en afspraken aantoonbaar kloppen voordat wordt gestart of opgeschaald.

De AI-verordening kent naast laag, beperkte en hoge risico's ook een categorie onaanvaardbaar *risico*: toepassingen die in de EU verboden zijn. Denk aan vormen van manipulatie, sociaal scoring door de overheid en bepaalde vormen van (massa)toezicht. Voor dit type geldt in Velsen: altijd NO-GO. De risicotriage in dit document (laag/beperkt/hoog) gaat dus over toepassingen die in principe wél binnen de kaders kunnen passen, afhankelijk van de borging. De zwaarste wettelijke eisen liggen vooral bij hoog risico systemen, daarom leggen we daar de lat hoger en vragen we meer aantoonbaarheid.

Belangrijk is dat dit niet alleen geldt voor nieuwe pilots. Ook bestaande systemen kunnen AI bevatten, inclusief ingekochte leverancierssoftware. Daarom geldt: bij relevante releases, nieuwe modules of contractwijzigingen wordt opnieuw beoordeeld of er AI is toegevoegd of uitgebreid. En wat dat betekent voor risico, transparantie, privacy en beveiliging. Zonder dit blijft de organisatie kwetsbaar doordat alleen nieuwe initiatieven worden getoetst, terwijl bestaande toepassingen buiten beeld blijven.

Generatieve AI

Het gebruik van generatieve AI zal naar verwachting toenemen, omdat het laagdrempelig is en direct waarde kan leveren in schrijven, samenvatten, voorbereiden en analyseren. Velsen wil die ontwikkeling benutten en de boot niet missen. Tegelijk is GenAI alleen verantwoord en schaalbaar als de basis op orde is: weten welke informatie in welke omgeving mag worden gebruikt, en dit ook kunnen afdwingen.

Als data-classificatie en technische handhaving (zoals toegangsrechten, labeling en waar passend DLP-maatregelen) niet of onvoldoende zijn ingericht, ontstaat een structureel risico: medewerkers gaan per team of persoon verschillende grenzen hanteren, terwijl de hoeveelheid AI-gebruik juist groeit. Dat vergroot de kans op onbedoelde datadeling, privacy-incidenten, onduidelijkheid over bewaartermijnen en beperkt de mogelijkheid om veilig op te schalen. Het gevolg is vaak dat de organisatie achteraf moet terugschakelen of beperkingen moet invoeren, waardoor innovatie vertraagt en vertrouwen afneemt.

Om dit risico te beheersen, werkt Velsen stapsgewijs toe naar organisatiebrede data-classificatie en technische handhaving bij GenAI (toegangsrechten, labeling en waar passend DLP). De concrete gebruiksregels en uitzonderingsroute zijn vastgelegd onder Basisregels en worden toegepast via de LITE- en DEEP-route.

Proces: Principes, LITE en DEEP scan

De kaders geven de norm. Het proces maakt het werkbaar. We werken met drie lagen. Zo wordt helder wat direct kan, wat eerst scherper moet en wat niet kan.

De organisatie werkt met 3 lagen toetsing.

De principes en kernwaarden vormen de voorkant. Dit is geschreven in gewone taal en is bedoeld om initiatiefnemers te helpen om doel, impact en verantwoordelijkheid helder te maken.

De LITE-check is de snelle intake die vooraf beoordeelt of een verzoek veilig kan starten. Doel en waarde worden scherp gezet, gegevensgebruik en noodzakelijkheid getoetst, het type AI benoemd en basisvoorwaarden voor transparantie en beveiliging gecontroleerd. De uitkomst is een beperkte pilot met borging, een vervolg naar verdieping of een afwijzing als randvoorwaarden ontbreken.

Daarom start elk initiatief met een scherp probleem, een duidelijke doelgroep en een kleine set indicatoren die je kunt volgen. We spreken minimaal één indicator af met een startwaarde, nulmeting waar mogelijk, en een streefwaarde. Geen meetbaar effect, dan geen opschaling en geen structurele inzet.

De DEEP-check wordt ingezet als LITE dat triggert, bijvoorbeeld bij impact op mensen, gevoelige data, hoog risico, of onduidelijke leveranciersvoorwaarden. In DEEP worden de privacy en juridische onderbouwing uitgewerkt, ethische aspecten (fairness en impact) onderzocht, robuustheid en veiligheid getest, transparantie vastgelegd en leveranciersafspraken geborgd. Het resultaat is een onderbouwd besluit met voorwaarden voor uitvoering en eventuele opschaling.

Initiatiefnemers staan hier niet alleen voor. We ondersteunen initiatiefnemers bij het invullen van de intake met voorbeelden en hulp vanuit privacy, security, inkoop of andere stakeholders. LITE en DEEP doen we altijd samen met de relevante stakeholders, zodat het geen solo-actie wordt maar een gezamenlijke toets.

Deze werkwijze sluit aan op de werkwijze van andere gemeentes: use-case kiezen, inrichten, monitoren en onderhouden. Daarmee wordt AI geen eenmalige beslissing, maar een beheerde toepassing die periodiek wordt beoordeeld.

Rollen, Mandaat en Besluitvorming

Voor succes is rolhelderheid essentieel. De initiatiefnemer dient het verzoek in en levert de inhoudelijke input. De proceseigenaar is de verantwoordelijke leidinggevende voor het proces/dienst, niet de initiatiefnemer. Ook als die rol niet formeel “product owner” heet, ligt hier het eigenaarschap: waarde, scope, acceptatiecriteria en het besluit om door te gaan of te stoppen.

De initiatiefnemer levert de eerste informatie aan, maar het eigenaarschap ligt bij de verantwoordelijke leidinggevende van het proces waar de AI in komt. Die eigenaar is aanspreekbaar op waarde, gebruik en besluitvorming. De informatieadviseur is vaak het eerste aanspreekpunt voor domeinen. Een initiatief om een AI-toepassing te verkennen of aan te schaffen kan daarom via deze route binnenkomen. De informatieadviseur helpt het verzoek scherp te krijgen en zorgt dat het initiatief in het juiste spoor landt. Als het initiatief gevolgen heeft voor systemen, gegevens of beheer, organiseert de informatieadviseur dat de juiste collega's aansluiten, zodat vanaf het begin duidelijk is wat nodig is en wat de randvoorwaarden zijn.

De Privacy Officers adviseren over grondslag, dataminimalisatie en privacyrisico's. De CISO adviseert over informatiebeveiliging, robuustheid, logging en incidentafhandeling. Architectuur toetst op inpasbaarheid en beheerbaarheid in het informatielandschap. Functioneel applicatiebeheer bewaakt de werking in de praktijk en signaleert wijzigingen (bijvoorbeeld AI-functionaliteit via updates) die herclassificatie of extra borging vereisen. Contractmanagement borgt dat afspraken over transparantie, auditbaarheid, dataverwerking, gebruik van output en exit ook contractueel kloppen. De Gegevensregisseur bewaakt herkomst, definities en kwaliteit van data. Bij hoog risico of grote impact is besluitvorming op hoger niveau logisch, bijvoorbeeld via de bestaande organisatiebrede intake of een vast overlegmoment.

Uit recente VNG-publicaties volgt dat gemeenten gebaat zijn bij één centraal, multidisciplinair aanspreekpunt voor AI en algoritmen. Zo'n kernteam bewaakt de risicoclassificatie, registratie en toetsing, ondersteunt proceseigenaren bij de LITE- en DEEP-route en adviseert over transparantie, privacy, informatiebeveiliging en bias. Het team rapporteert periodiek over gebruik, incidenten, bevindingen en verbeteracties, zodat bestuur en management aantoonbaar ‘in control’ blijven. Deze inrichting sluit aan op VNG-aanbevelingen over centraal eigenaarschap, duidelijke verantwoordelijkheden en auditbaarheid. Op basis hiervan kan worden beoordeeld of en hoe dit model binnen Velsen gewenst en haalbaar is.

Capaciteit en Middelen

Deze aanpak vraagt tijd en rolverdeling. Zonder capaciteit wordt het beleid een papieren werkelijkheid of ontstaat wachttijd die innovatie remt.

In de startfase is een lichte, maar vaste inrichting nodig. Denk aan een coördinerende rol die intake, registratie en kennisdeling organiseert en die de koppeling met het bestaande tool intakeproces bewaakt. Daarnaast is structurele beschikbaarheid nodig van Privacy Officers, CISO en de gegevensregisseur voor toetsing en advies. De proceseigenaren in de lijn moeten tijd reserveren om doelen, KPI's, acceptatiecriteria en evaluaties te borgen.

Het gaat niet om een nieuw “AI-bureau”, maar om heldere rolafspraken en uren die expliciet worden vrijgemaakt. Daarmee wordt voorkomen dat pilots blijven hangen of dat risico's pas laat in beeld komen.

Inkoop en leveranciers als kernonderdeel

Veel AI komt via leveranciers. Daarom horen leverancierseisen bij de kern van de kaders. Afspraken moeten gaan over datagebruik, bewaartermijnen, hergebruik van input, auditrechten, exit en ondersteuning bij incidenten. Zonder dit kan de gemeente niet aantonen dat zij in control is.

Daarom nemen we in het inkoopproces vaste AI-eisen op. De leverancier:

- bevestigt of de oplossing AI bevat, welke functionaliteiten dat zijn en in welke risicoklasse het valt;
- levert bij hoog risico de benodigde onderbouwing voor naleving van de AI verordening en geeft aan wie welke verplichting draagt;
- meldt bij elke release, nieuwe module of contractwijziging of AI is toegevoegd of uitgebreid, en of dat de risicoklasse wijzigt;
- geeft inzicht in dataverwerking, bewaartermijnen, hergebruik van input en output, auditrechten, incidentondersteuning en een werkbare exit.

Dit sluit aan bij de landelijke beweging richting collectieve afspraken en standaarden. Waar mogelijk wordt aangesloten op gezamenlijke kaders om versnippering en dubbele compliance inspanning te voorkomen.

Transparantie en communicatie richting inwoners

Transparantie is geen abstract ideaal, maar een bestuurlijke en wettelijke verplichting. Het hangt samen met zorgvuldigheid, uitlegbaarheid, gelijke behandeling en een goede motivering van keuzes. Medewerkers moeten weten wanneer AI gebruikt mag worden en hoe zij dat veilig doen. Inwoners moeten kunnen herkennen wanneer AI wordt ingezet en wat dat betekent. Bij toepassingen met impact hoort ook een route voor vragen, bezwaar en herstel.

Daarom wordt bij relevante toepassingen een begrijpelijke toelichting opgesteld die in het algoritmeregister wordt gepubliceerd. Dit is een belangrijk onderdeel van publiek vertrouwen, zeker in het sociaal domein.

Registratie en overzicht horen daarbij. Voor hoog risico AI-systemen die onder Annex III van de AI-verordening vallen, geldt registratie in de EU-database. De leverancier registreert het systeem. Velsen registreert als publieke organisatie ook het gebruik van het systeem. Voor lage en beperkte risico's geldt in de AI-verordening geen algemene registratieplicht. We houden intern wel een actueel overzicht bij van welke AI we gebruiken, in welke risicoklasse het valt en welke borging daarbij hoort, zodat het gebruik controleerbaar blijft en we kunnen verantwoorden wat we doen en waarom.

Privacy, informatiebeveiliging en ethiek

Privacy, informatiebeveiliging en ethiek zijn een dragende pijler onder verantwoord gebruik van AI. Velsen werkt daarom vanuit het principe: veilig en rechtmatig by design. Niet achteraf. Deze aanpak sluit aan op bestaande werkwijzen en kaders, zoals de AVG voor persoonsgegevens en de BIO en NIS2 (Cyberbeveiligingswet) voor digitale veiligheid. Deze aanpak moet daarom ook in samenhang met het privacy- en informatiebeveiligingsbeleid worden gelezen. De privacy officers en CISO hebben een belangrijke rol bij het innoveren met AI.

Vertrouwen is een randvoorwaarde. Dat betekent zorgvuldig omgaan met privacy en persoonsgegevens, dataminimalisatie als uitgangspunt en heldere afspraken over bewaartermijnen en verwijdering. We hebben ook aandacht voor gelijkheid. Als AI mensen kan raken, kijken we actief naar risico's op uitsluiting of vertekening en leggen we vast hoe herstel plaatsvindt als er toch nadeel ontstaat.

Veiligheid en betrouwbaarheid horen bij het ontwerp. AI-toepassingen moeten bestand zijn tegen fouten, misbruik en onverwacht gedrag. Velsen wil kunnen terugschakelen als kwaliteit onder de norm zakt, of als er signalen zijn dat de toepassing onveilig of onbetrouwbaar is.

Wat we verstaan onder de norm leggen we per toepassing vooraf vast, bij voorkeur op basis van de risicoklasse. We bepalen welke minimale kwaliteit nodig is, welke foutmarge acceptabel is en wanneer we terugschakelen of stoppen.

Concreet betekent dit dat elk AI-initiatief expliciet maakt welke gegevens worden gebruikt, wat de grondslag is, welke risico's er zijn en hoe die risico's worden beperkt. Waar nodig zetten we bestaande instrumenten in, zoals DPIA's, verwerkersafspraken, beveiligingsmaatregelen, logging en monitoring, en afspraken over incidentmelding, audit en exit. Generatieve AI kent specifieke misbruikscenario's, zoals prompt-injection en onbedoelde datalekken via gekoppelde bronnen (bijvoorbeeld documenten en samenwerkingsomgevingen). Daarom worden toepassingen bij voorkeur in een beheerde omgeving aangeboden, met passende toegangsrechten, scheiding van gevoelige bronnen, logging en monitoring. Bij signalen van misbruik, datalekken of kwaliteitsproblemen geldt dat wordt teruggedraaid naar een veilige werkwijze

(fallback) en waar nodig wordt teruggedraaid naar een eerdere, stabiele situatie of versie (rollback), volgens de afgesproken incidentprocedure.

De AI-checks (LITE en DEEP) maken dit werkbaar. LITE borgt dat pilots alleen starten als de basisvoorwaarden voor privacy, informatiebeveiliging en transparantie op orde zijn. DEEP zetten we in bij hogere risico's of impact op inwoners. Daarmee zorgen we voor aantoonbare onderbouwing, bewijsstukken en heldere verantwoordelijkheden, voordat we starten of opschalen. Bij toepassingen met hogere impact kan een onafhankelijke ethische toets onderdeel zijn van de DEEP-route. Het advies wordt betrokken bij het stop of door besluit door de proceseigenaar en de verantwoordelijke besluitlijn voor pilots en opschaling. Zo is de ethische afweging expliciet en aantoonbaar, zonder dat dit een parallel traject wordt.

Naast privacy en informatiebeveiliging is ook ethiek, en specifiek data-ethiek, een belangrijk onderdeel van verantwoord AI-gebruik. Bij data-ethiek gaat het niet alleen om wat technisch mogelijk is of wat wettelijk mag, maar vooral om wat eerlijk is voor onze inwoners. Het draait om vragen als: Willen we dit wel? Past dit bij onze waarden? Het gebruik van AI brengt nieuwe kansen, maar ook dilemma's. Daarom werken we ernaartoe om een externe ethische commissie op te richten. Dit is een belangrijke stap om de integriteit en transparantie binnen onze gemeente te waarborgen. Door AI-vraagstukken voor te leggen aan een onafhankelijke externe ethische commissie zorgen we voor een objectieve blik van buitenaf. Dit voorkomt dat we alleen vanuit onze eigen organisatie redeneren en helpt ons om verantwoorde keuzes te maken. Zo laten we zien dat we zorgvuldig omgaan met de inzet van AI en data én kunnen we verantwoord innoveren.

AI en architectuur

Net zoals andere onderdelen van ons informatielandschap moeten ook AI-onderdelen getoetst worden aan de architectuurprincipes die we voor dit landschap hebben opgesteld en vastgesteld. Zijn er AI-onderdelen die niet aan deze principes voldoen maar willen we ze toch gebruiken, dan geven we aan waarom we dit doen en leggen we dit vast. De toetsing van deze principes vindt al plaats in de bestaande organisatiebrede intake waar eerder in dit document al aan gerefereerd is, dus daar hoeft niets nieuws voor ingericht te worden. Vanwege de razendsnelle ontwikkeling van AI is het wel nodig om de vastgestelde architectuurprincipes kritisch onder de loep te nemen en, daar waar nodig, aan te passen of aan te vullen. Ook kan overwogen worden om specifieke afgeleide principes op te stellen voor AI mocht dat wenselijk zijn.

Daarnaast zijn er technische ontwikkelingen die inspelen op de snelle ontwikkeling van AI, denk hierbij aan PC's die speciaal zijn geconfigureerd voor het optimaal (lokaal) gebruik van AI. Deze ontwikkelingen moeten meegenomen worden in de keuze hoe we AI willen gaan gebruiken.

Adoptie en AI-geletterdheid: van beleid naar gedrag

AI-beleid werkt alleen als medewerkers weten wat verantwoord is. Training is daarom niet voldoende als losse actie. Er is ook ondersteuning nodig in de werkpraktijk: korte richtlijnen, voorbeeldcasussen, een vaste route voor vragen en een duidelijk proces voor pilots.

De ambitie om medewerkers te enthousiasmeren en het gebruik te vergroten is haalbaar, mits het gebruik wordt gekoppeld aan veilige werkwijzen en duidelijke randvoorwaarden. De organisatie leert via pilots, verwerkt lessen in richtlijnen, en scherpt waar nodig processen en checklists aan.

Om dit beleid in de praktijk te laten werken is één ding cruciaal: collega's moeten weten waar ze terecht kunnen en wat de route is, terwijl privacy en security niet pas achteraf in beeld komen. De organisatie kan dit simpel houden door aan te sluiten op wat er al is. De bestaande organisatiebrede intake voor aanschaf en inzet van informatieproducten blijft het centrale kanaal. De AI-principes en de LITE- en DEEP-check worden daar stapsgewijs aan gekoppeld, zodat AI geen parallel traject wordt en besluitvorming op één plek blijft landen.

In de startfase is het logisch om de AI-checks primair te gebruiken voor pilots en sandboxing. Niet omdat structurele inzet onbelangrijk is, maar omdat pilots de meeste onzekerheid bevatten en de meeste leerwaarde opleveren. Door pilots standaard te laten beginnen met een korte principetoets en een LITE-check, ontstaat snel een uniform minimum. Wanneer de LITE-check signalen geeft van hogere impact of gevoelige data, volgt automatisch de DEEP route. Daarmee wordt de inspanning proportioneel: licht waar het kan, zwaar waar het moet.

De rolverdeling moet expliciet worden gemaakt, anders verdwijnt het werk tussen wal en schip. Een belangrijk punt is capaciteit. Dit werkt alleen als er tijd wordt vrijgemaakt voor intake, toetsing en begeleiding. Niet als groot programma, maar als structurele uren in bestaande rollen. Zonder die uren wordt de keuze feitelijk: of innovatie vertraagt, of risico's schuiven door naar later. Door vooraf capaciteit te reserveren voor beoordeling en borging, blijft het tempo hoog en blijven beslissingen uitlegbaar.

Voor medewerkers is de belangrijkste succesfactor dat de werkwijze simpel en herkenbaar is. Dat vraagt om één duidelijke set richtlijnen voor generatieve AI in het dagelijks werk, één plek waar vragen en voorbeelden samenkomen, en een korte uitleg van wat wel en niet kan met gegevens. Zo voorkom je dat iedereen het wiel opnieuw uitvindt of uit onzekerheid helemaal stopt. Het helpt ook om managers dezelfde taal te geven: wat is publieke waarde, wat is acceptabel risico, en wanneer is verdieping nodig.

Voor de technische basis geldt hetzelfde principe: klein beginnen, maar wel in een gecontroleerde omgeving. De organisatie hoeft niet direct een groot platform te bouwen,

maar wel een veilige standaardroute te organiseren voor pilots. Dat betekent dat er een afgesproken toolset is, dat toegang is geregeld, en dat vastligt hoe gegevens worden verwerkt en verwijderd. Zodra pilots vaker voorkomen, wordt het verstandig om die basis verder te professionaliseren, zodat experimenteren niet afhankelijk is van losse technische keuzes per team.

Tot slot hoort bij volwassen AI gebruik dat het leren wordt vastgelegd. Een pilot ‘slaagt’ ook als blijkt dat een toepassing (op dit moment) niet werkbaar, niet bruikbaar of niet verantwoord is. Dat levert juist waardevolle leerpunten op. Elke pilot levert niet alleen een uitkomst op, maar ook inzichten over risico’s, randvoorwaarden en wat wel of niet werkt. Door die inzichten terug te laten vloeien in de richtlijnen, de checklists en de inkoopafspraken, wordt het beleid elk kwartaal sterker zonder dat het zwaarder wordt. Zo ontstaat een praktische cyclus: leren, aanscherpen en gecontroleerd opschalen.

Afsluiting

De kern van deze aanpak is dat AI niet wordt behandeld als een losse innovatie, maar als een onderdeel van de organisatiestrategie. Dat maakt het mogelijk om kansen te benutten en tegelijk publieke waarden te beschermen. Door AI te zien als intensieve automatisering ontstaat een duidelijke focus: ondersteuning van medewerkers, verbetering van dienstverlening en meetbare waarde in processen. Tegelijk wordt voorkomen dat de organisatie afhankelijk wordt van ad-hoc keuzes, schaduwgebruik of leverancierslogica.

Deze aanpak combineert snelheid met zorgvuldigheid. De principes en kernwaarden bieden richting in gewone taal. De LITE-check maakt snelle, veilige pilots mogelijk. De DEEP-check borgt dat zwaardere toepassingen aantoonbaar kloppen op privacy, veiligheid, transparantie en verantwoordelijkheid. Dat is nodig om vertrouwen te behouden, om bestuurlijk uit te kunnen leggen waarom iets wel of niet kan, en om later niet te worden verrast door juridische of ethische issues.

Belangrijk is dat dit geen parallel circuit wordt. Velsen heeft al een organisatiebreed intakeproces voor aanschaf en inzet van tools. De AI-checks zijn zo ingericht dat ze hierop kunnen aansluiten, zodat AI uiteindelijk een vaste kwaliteitstoets wordt in normale besluitvorming. Dat vraagt rolhelderheid, vaste overlegmomenten en expliciete inzet van capaciteit. Niet omdat er een nieuw “AI-bureau” nodig is, maar omdat toetsing, registratie, begeleiding en evaluatie tijd kosten en eigenaarschap vragen.

Uiteraard zou de organisatie een vaste ritmiek moeten inrichten voor evaluatie en bijsturing, omdat technologie, wetgeving en leveranciers blijven veranderen. Voor generatieve AI is daarbij één randvoorwaarde essentieel: data-classificatie en technische handhaving. Omdat GenAI-gebruik naar verwachting toeneemt, is verantwoord opschalen alleen mogelijk als helder is welke informatie in welke omgeving mag worden gebruikt en dit ook wordt afgedwongen met toegangsrechten, labeling en waar passend DLP. Totdat dit organisatiebreed op orde is, blijft GenAI beperkt tot niet-vertrouwelijke informatie en generieke taken; uitzonderingen zijn alleen mogelijk via expliciete toetsing en vastlegging van maatregelen.

Pilots en live toepassingen zouden periodiek beoordeeld moeten worden op waarde, kwaliteit, incidenten en naleving, waarna richtlijnen, checklists en inkoopafspraken worden aangescherpt. Ook AI-geletterdheid zou doorlopend aandacht moeten krijgen, met basisinstructie voor nieuwe collega's en korte praktijkopfrissingen voor teams. Zo blijft de werkwijze actueel en veilig, zonder dat de organisatie telkens opnieuw het wiel hoeft uit te vinden.

Met deze lijn kan Velsen veilig experimenteren en gecontroleerd opschalen. De organisatie leert met echte casussen, bouwt aantoonbare borging op, en kan keuzes maken op basis van feiten in plaats van gevoel. Zo blijft de gemeente in control, ook als de technologie zich snel ontwikkelt, en ontstaat er ruimte om AI duurzaam in te zetten waar het echt waarde toevoegt.

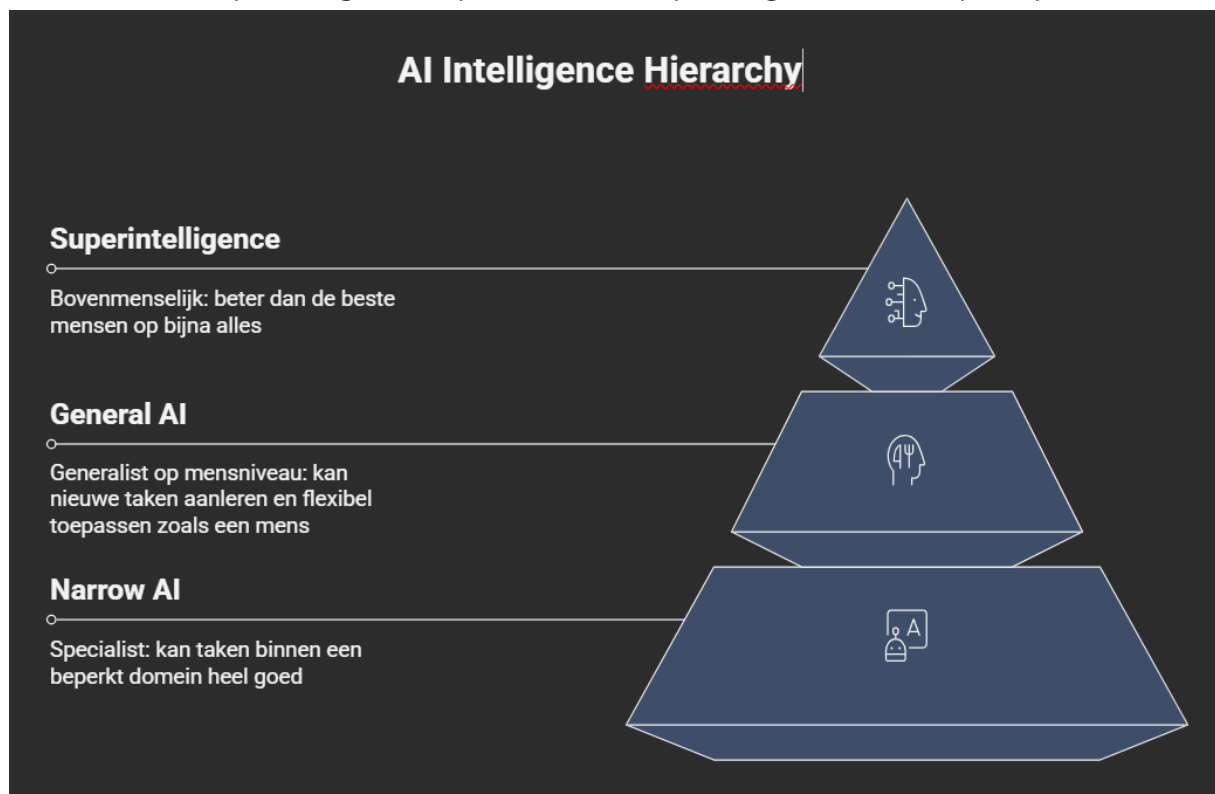
Bijlage A: Begrippenlijst

Begrip	Uitleg
AI	Verzamelnaam voor systemen die taken uitvoeren die normaal menselijke intelligentie vragen, zoals herkennen, voorspellen, genereren of adviseren.
Generatieve AI	AI die nieuwe tekst, beelden of samenvattingen kan maken, bijvoorbeeld voor conceptteksten of spraak naar tekst.
Classificerende of voorspellende AI	AI die patronen herkent en een label of inschatting geeft, bijvoorbeeld een risico indicatie of categorie.
Menselijk toezicht	Een medewerker blijft verantwoordelijk, kan ingrijpen en kan de inzet of uitkomst corrigeren, zeker wanneer mensen geraakt worden.
Publieke waarde	Aantoonbare verbetering voor inwoners, medewerkers of de organisatie, zoals kwaliteit, snelheid, toegankelijkheid, of doelmatigheid.
Proportionaliteit	Dit betekent dat er een redelijke verhouding moet zijn tussen het doel en het ingezette middel. Het lichtst passende middel heeft de voorkeur; als een eenvoudiger oplossing hetzelfde bereikt, is die leidend.
AI verordening (AI Act)	Europese wet die AI indeelt naar risico en verplichtingen stelt voor veiligheid, transparantie en beheersing.
Risicoklassen (laag, beperkt, hoog)	Praktische indeling die bepaalt welke borging nodig is. Hoe dichterbij besluitvorming of inwonerimpact, hoe zwaarder de eisen.
Risicotriage	Praktische inschatting van laag, beperkt of hoog risico om te bepalen of LITE volstaat of DEEP verplicht is.
LITE-check	Snelle intake voor pilots die toetst of een initiatief veilig kan starten met basisborging.
DEEP-check	Verdiepende beoordeling met bewijsstukken en afspraken, nodig bij hogere risico's of grotere impact.
Terugvalopties (fallback/rollback)	Afspraken over terugschakelen naar handmatig/vaste werkwijze (fallback) en terugdraaien naar een eerdere, veilige situatie of versie (rollback) bij fouten of incidenten.
Logging en monitoring	Logging: vastleggen van relevant gebruik en gebeurtenissen. Monitoring: actief volgen van kwaliteit/afwijkingen zodat tijdig kan worden ingegrepen.
Algoritmeregister	Registratie en uitleg van relevante algoritmen of AI-toepassingen, zodat gebruik transparant en controleerbaar is.
Algoritme	Een set van regels en instructies die een computer geautomatiseerd volgt bij het maken van berekeningen om een probleem op te lossen of een vraag te beantwoorden.

Sandbox	Gecontroleerde omgeving waarin pilots kunnen draaien met duidelijke grenzen, zodat leren mogelijk is zonder onnodige risico's.
Machine learning	Technieken waarbij systemen leren van voorbeelden in data in plaats van vaste regels.
Deep learning	Onderdeel van machine learning met neurale netwerken, sterk in taal/beeld/spraak; basis onder veel GenAI-toepassingen.
DLP (Data Loss Prevention)	Technische maatregelen die onbedoeld delen/lek blokkeren of signaleren.
Prompt-injection	Manipulatie van instructies waardoor een model ongewenst gedrag vertoont of data prijsgeeft.
DPIA	Een Data Protection Impact Assessment (DPIA) is een verplicht instrument onder de AVG om privacyrisico's bij gegevensverwerking in kaart te brengen en te minimaliseren.

Bijlage B: AI

AI is een verzamelnaam voor systemen die taken uitvoeren of ondersteunen op basis van data. Onder de paraplu van AI wordt vaak een indeling gebruikt in drie niveaus, zie figuur 1 Narrow AI (ANI), Artificial General Intelligence (AGI) en Artificial Superintelligence (ASI). De toepassingen die nu in de praktijk relevant zijn, vallen vrijwel altijd onder Narrow AI (ANI). Voor Velsen betekent dit dat AI-toepassingen vooral één afgebakende taak ondersteunen. Binnen Narrow AI vallen generatieve toepassingen (GenAI) en voorspellende of classificerende toepassingen. Ook besluit- of procesondersteuning en andere vormen van datagedreven ondersteuning vallen hieronder. Het gaat om ondersteunende toepassingen, niet om systemen die breed kunnen redeneren of autonoom besluiten nemen. Daarom zijn de kaders en de toetsing in dit document primair gericht op Narrow AI-toepassingen in de werkpraktijk.



Figuur 1: Hierarchie van AI Intelligence

Figuur 1: Artificial Intelligence Hiërarchie

Voorbeelden om de niveaus te begrijpen:

Narrow AI (ANI)

Een systeem dat Wmo-aanvragen automatisch indeelt en ondersteunt. Het herkent uit de tekst waar de aanvraag over gaat, bijvoorbeeld hulp bij huishouden, begeleiding of hulpmiddelen, en zet deze in de juiste werkbak. In de praktijk kan dit zowel regelgebaseerd (vaste proceslogica) als met een vooraf getraind model (bijvoorbeeld

tekstclassificatie) worden gerealiseerd. Zulke modellen worden vaak vooraf getraind en hoeven tijdens gebruik niet continu bij te leren. Het kan ontbrekende informatie signaleren, zoals missende bijlagen, en een standaardbericht klaarzetten. Daarnaast kan het een voorspelling doen, bijvoorbeeld een inschatting van urgentie of de verwachte doorlooptijd op basis van eerdere, vergelijkbare aanvragen. In de praktijk is dit vaak een combinatie van tekstverwerking, patroonherkenning en proceslogica die de volgende stap voorbereidt.

Artificial General Intelligence (AGI)

De medewerker zegt: “Breng de belangrijkste oorzaken van lange doorlooptijden in het Wmo aanvraagproces in kaart en maak een verbeterplan.” Het systeem haalt data uit verschillende bronnen, bouwt een passend datamodel, analyseert waar vertraging ontstaat, bijvoorbeeld in triage, in het opvragen en verwerken van aanvullende informatie, of leveranciersprocessen, doet voorstellen per stap, rekent effecten door op wachttijd en kosten, en schrijft een adviesnotitie plus een dashboard-opzet. De medewerker beoordeelt en stuurt bij, maar het systeem kan de klus grotendeels zelfstandig uitvoeren.

Vandaag kunnen combinaties van ANI-toepassingen en geautomatiseerde workflows al onderdelen van dit soort opdrachten ondersteunen. Het verschil met AGI is dat betrouwbaarheid, contextbegrip en zelfstandige generalisatie nog niet op mensniveau zijn. Daardoor blijven structureel toezicht en verificatie noodzakelijk.

Artificial Superintelligence (ASI)

Het systeem ontdekt niet alleen knelpunten, maar ontwerpt een compleet nieuwe aanpak die beter werkt dan wat teams normaal bedenken. Bijvoorbeeld: het simuleert duizenden scenario's voor intake, prioritering, inzet van consultants en contractering met aanbieders, en vindt een combinatie die wachttijden sterk verlaagt zonder dat kwaliteit of rechtmatigheid daalt. Het komt met argumenten, risico's en een uitvoerbare routekaart die op vrijwel alle punten sterker is dan menselijke plannen.

Voor AGI en ASI bestaat geen breed gedragen, concrete planning. In discussies worden soms jaartallen genoemd richting 2040, maar die zijn speculatief. Wel is duidelijk dat naarmate systemen krachtiger en zelfstandiger worden, de eisen aan menselijk toezicht, governance, transparantie en beheersing toenemen. Daarom is “in control blijven” geen eenmalige keuze, maar een structurele opgave die meegroeit met de technologie.

Bijlage C: AI Vandaag

Binnen de ANI-fase komen grofweg drie vormen voor. Ze verschillen vooral in wat ze opleveren: een tekstvoorstel, een inschatting of label, of een concreet advies voor de volgende processtap. In de praktijk zijn dit geen losse “hokjes”, maar bouwstenen die vaak in een toepassing worden gecombineerd.

Generatieve AI (GenAI)

GenAI maakt, herschrijft of vat content samen. Denk aan tekst, samenvattingen, conceptantwoorden, vertalingen, spraak-naar-tekst en ook beeld, audio en video. Toepassingen zoals ChatGPT, Copilot en Gemini vallen hieronder. Ook grote zoekmachines gebruiken steeds vaker GenAI om zoekresultaten samen te vatten of direct antwoord te geven. In de praktijk werkt GenAI vooral goed als hulpmiddel voor medewerkers, bijvoorbeeld voor het samenvatten van een dossier, het opstellen van een conceptbericht of het sneller terugvinden van kernpunten. De uitkomst blijft een voorstel en vraagt altijd om inhoudelijke controle.

Voorspellende of classificerende AI

Deze vorm herkent patronen in data en geeft een inschatting of label terug. Voorbeelden zijn een risicoscore, prioritering, signalering van afwijkingen, of een indeling in categorieën, zoals het type aanvraag of de kans op heraanvraag. Dit soort modellen werkt meestal met gestructureerde gegevens en historische voorbeelden. Betrouwbare inzet vraagt daarom niet alleen goede data, maar ook duidelijke processen voor beheer, monitoring en periodieke herbeoordeling. De kwaliteit is afhankelijk van datakwaliteit, representativiteit en het voorkomen van ongewenste vertekening.

Besluit en proces ondersteunende systemen

Dit zijn systemen die een besluit voorbereiden of deels automatiseren. Ze combineren regels, beleidslogica en soms modellen tot een voorstel voor de volgende stap, bijvoorbeeld een adviesroute, een controlelijst, een voorgestelde planning of een conceptbesluit met toelichting. Dit is vaak geen zelfstandig besluit, maar een hulpmiddel dat consistentie en snelheid kan vergroten, mits rollen, verantwoordelijkheden en controlemomenten helder zijn ingericht.

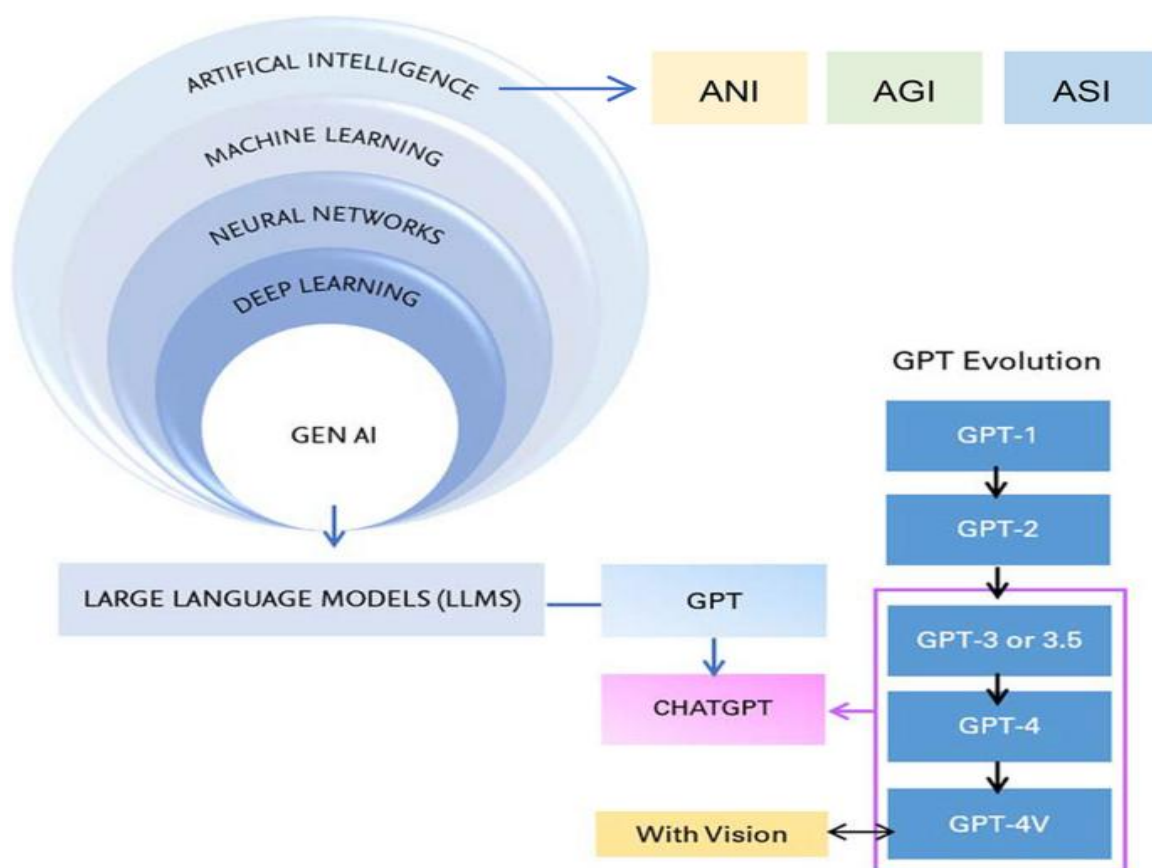
In de praktijk worden deze vormen vaak gecombineerd. Een systeem kan bijvoorbeeld tekst analyseren en samenvatten, daarna labels of signalen toevoegen en vervolgens een voorstel klaarzetten voor de volgende processtap. Juist bij zulke combinaties is het belangrijk om vooraf helder te maken wat het systeem mag doen, wat de medewerker altijd moet controleren en hoe afwijkingen en fouten worden opgevangen.

Begrippen in gewone taal

Wat we nu in de praktijk vooral tegenkomen, zoals toepassingen voor tekst, beeld, video en spraak, valt vrijwel altijd onder de fase Narrow AI (ANI). Deze ontwikkelingen vormen belangrijke bouwstenen voor mogelijke vervolgstappen richting AGI en ASI.

In de praktijk worden termen als AI, machine learning en generatieve AI vaak door elkaar gebruikt. Toepassingen zoals ChatGPT, Copilot en Gemini werken met taalmodellen, vaak in de vorm van een Large Language Model (LLM). Een LLM is een type generatieve AI en valt daarmee binnen de ANI-fase. Het kan nieuwe tekst maken, samenvatten en vragen beantwoorden op basis van patronen die het heeft geleerd uit grote hoeveelheden tekst. Generatieve AI is breder dan taal: er bestaan ook generatieve modellen voor beeld, audio en video.

Machine learning is de verzamelnaam voor technieken waarbij systemen leren van voorbeelden in data. Deep learning is een onderdeel daarvan en gebruikt neurale netwerken die vooral goed werken bij taal, beeld en spraak. Een LLM is in de basis een deep learning-model en valt daarmee onder machine learning, zoals schematisch weergegeven in figuur 2.



Figuur 2 AI Taxonomie

Deze technieken vormen vaak de basis van ANI-toepassingen en zullen waarschijnlijk ook in de toekomst belangrijke bouwstenen blijven, naast nieuwe technieken die nog worden ontwikkeld.

Bijlage D: Algoritmes en AI in software

In de gemeentelijke praktijk wordt ook vaak gesproken over algoritmes. Daarmee wordt bedoeld: de logica die bepaalt hoe een systeem tot een uitkomst komt. Dat kan heel simpel zijn, zoals vaste beslisregels, maar ook complex, zoals een (vooraf)getraind model. Belangrijk aandachtspunt is dat AI soms “verstoep” zit in leverancierssoftware of nieuwe updates, ook als het niet expliciet zo wordt genoemd. Daarom is het nodig om alert te zijn op AI-functionaliteit in bestaande systemen, bij uitbreidingen en bij grote releases.

Bijlage E: Rollen AI

De technologie ontwikkelt snel en toepassingen worden zelfstandiger. In de praktijk beweegt AI grofweg langs drie rollen.

- Eerst als inzicht-tool: het systeem helpt met zoeken, ordenen, samenvatten en signaleren.
- Daarna als co-piloot: het systeem doet voorstellen, maakt concepten en ondersteunt een medewerker stap-voor-stap, terwijl de medewerker aan het stuur blijft.
- De volgende stap is auto-piloot: het systeem voert meerdere stappen zelfstandig uit, bijvoorbeeld informatie ophalen, verwerken en een vervolgactie klaarzetten.

Hoe verder richting auto-piloot, hoe belangrijker het wordt om menselijk toezicht, grenzen en terugvalopties vooraf strak te regelen. Dit document kiest bewust voor tempo mét controle: ruimte voor inzicht-tools en co-piloot-toepassingen, en pas richting auto-piloot als doel, risico's, gegevensbescherming en governance aantoonbaar op orde zijn.

Wat AI onderscheidt van gewone automatisering is dat het systeem niet alleen regels afloopt, maar ook met een bepaalde mate van autonomie werkt. Het leidt uit input af hoe het output maakt (zoals voorspellingen, aanbevelingen of tekst). Sommige AI-systemen kunnen zich na ingebruikname ook aanpassen, bijvoorbeeld doordat instellingen, data of context veranderen. Daarom is “in control blijven” geen eenmalige check, maar iets dat je tijdens gebruik blijft borgen. De kern blijft hetzelfde: hoe slimmer en autonomer een systeem wordt, hoe belangrijker het is dat de organisatie grip houdt op doel, data, risico's en menselijk toezicht.

Bijlage F: Framework for Trustworthy AI

A1 - Mens-centraal

(mens behoudt regie, geen automatisering van finale besluiten zonder toezicht)

- Wie neemt uiteindelijk de beslissing?
- Wanneer grijpt een mens in als het advies twijfel is of afwijkt?
- Kan een medewerker het systeem pauzeren/stoppen en staat dat ergens beschreven?

A2 - Proportionaliteit

(AI is een middel, geen doel; is er een eenvoudiger alternatief?)

- Is er een eenvoudiger oplossing dan AI geprobeerd of bekeken?
- Wat levert dit op en is dat in verhouding tot de moeite/kosten?
- Wat doen we juist niet met deze oplossing (afbakening)?

A3 - Fairness / non-discriminatie

(risico op bias/subgroepen?)

- Kan een bepaalde groep hier nadeel van krijgen? Welke?
- Hoe controleren we of de uitkomst voor groepen niet scheef is (bijv. steekproef/vergelijking)?
- Wat is de route voor herstel als iemand ongelijk is behandeld?

A4 - Transparantie & uitlegbaarheid

(kunnen we begrijpelijk uitleggen wat AI wel/niet doet?)

- Kunnen we uitleggen wat de AI wel/niet doet voor de gebruiker??
- Weten gebruikers dat er AI is gebruikt en waar staat die uitleg?
- Is er een korte tekst klaar voor de website/het algoritmeregister?

A5 - Privacy & dataminimalisatie

(minimale, passende data; grondslag helder)

- Welke gegevens gebruiken we en kan dat met minder?
- Waarom mag dit volgens de privacyregels (welke reden/grondslag)?
- Zitten er gevoelige gegevens in (bv. gezondheid, geloof, BSN)? Zo ja, echt nodig?

A6 - Robuustheid & veiligheid

(fouten/aanvallen, fallback/rollback)

- Wanneer vinden we de uitkomst “goed genoeg” (afgesproken kwaliteit)?
- Wat doen we als de uitkomst niet goed is of het systeem uitvalt (terug naar handmatig/vaste werkwijze)?
- Wie krijgt toegang en wordt het gebruik bijgehouden (logboek)?

- Welke beveiligingsmaatregelen zijn er getroffen?

A7 – Accountability

(eigenaar & besluitvorming duidelijk)

- Wie is eigenaar en mag “ja/nee” zeggen?
- Waar leggen we beslissingen en uitzonderingen vast?
- Wie houdt wijzigingen bij en plant een herbeoordeling?
- Uit welk budget wordt dit betaald?
- Geef een inschatting van eventuele kosten