gemeente Hollands Kroon

GEMEENTEBLAD

Officiële uitgave van de gemeente Hollands Kroon

Nr. 133793

23 maart

2026

Strategisch AI-Beleid

Managementsamenvatting

Wat is het doel van het beleid?

Het AI-beleid van de gemeente Hollands Kroon biedt een strategisch kader voor het verantwoord en transparant inzetten van kunstmatige intelligentie (AI).

Het beleid heeft drie subdoelen:

1. **Verbetering van de dienstverlening**: Door AI in te zetten, streeft de gemeente naar een hogere kwaliteit en toegankelijkheid van haar diensten voor zowel inwoners als bedrijven. Hierbij wordt strikt rekening gehouden met informatiebeveiliging, privacy en mensenrechten;
2. **Efficiëntere bedrijfsvoering**: AI wordt gebruikt om de interne processen te optimaliseren, besluitvorming te ondersteunen met data-analyse, en medewerkers te trainen in het gebruik van AI-technologieën.
3. **Borgen van verantwoord gebruik**: Met het oog op transparantie en veiligheid richting inwoners en diens gegevens.

Belangrijkste aspecten

- **Transparantie**: Alle AI-gebruik wordt geregistreerd en openbaar gemaakt om transparantie te waarborgen.
- **Menselijke controle**: Besluitvorming ondersteund door AI blijft altijd onder menselijke supervisie om ethische en verantwoorde beslissingen te garanderen.
- **Privacybescherming**: AI-systemen worden ontworpen en ingezet met inachtneming van strikte privacyregels om de gegevens van inwoners te beschermen.
- **Naleving van wet- en regelgeving**: Het beleid zorgt ervoor dat alle AI-toepassingen voldoen aan de relevante wet- en regelgeving, zoals de AI Act en de AVG.

Inleiding

Wat is Kunstmatige intelligentie (AI)

Een AI-systeem is een technologie die zelfstandig gegevens verwerkt en gebruikt om taken uit te voeren waarvoor normaal gesproken menselijke intelligentie nodig is. Het systeem analyseert data, herkent patronen en leert zelfstandig van nieuwe informatie. Hierdoor kan het zelfstandig complexe beslissingen nemen en voorspellingen doen. AI werkt als een 'slimme' software die op basis van data leert en handelt, eventueel zonder directe menselijke tussenkomst.

Kunstmatige intelligentie (AI) binnen Hollands Kroon

Kunstmatige intelligentie (AI) biedt kansen voor Hollands Kroon om als overheid slimmer, efficiënter en effectiever te werken. AI helpt bij het automatiseren van processen, het analyseren van grote hoeveelheden gegevens en het ondersteunen van besluitvorming. Binnen onze organisatie kan AI worden ingezet voor toepassingen zoals het verbeteren van de dienstverlening aan inwoners, het doen van voorspellingen bij beleidsvorming, het slim beheren van infrastructuur en fraudedetectie.

In lijn met onze i-visie 2024-2028 ondersteunt de inzet van AI het realiseren van producten en diensten die aansluiten bij de behoeften van onze inwoners. AI is daarbij geen doel op zich, maar een middel om onze processen en dienstverlening te versterken.

Reikwijdte van het beleid

Dit strategisch beleid is van toepassing op:

- Alle teams en medewerkers van de gemeente
- Zowel intern ontwikkelde als extern geleverde AI-systemen
- Alle fasen van AI-implementatie: van ontwikkeling tot uitfasering
- Samenwerkingen met externe partijen op het gebied van AI

Evaluatie en herziening

Het beleid wordt jaarlijks geëvalueerd door de Chief AI Officer (CAIO), Privacy officer (PO)/ Chief information security officer (CISO), Chief Data Officer (CDO). Het beleid wordt indien nodig opnieuw vastgesteld vanwege de snelle ontwikkelingen in AI.

Visie

Gemeente Hollands Kroon wil kunstmatige intelligentie op een slimme en integere manier gebruiken om de dienstverlening en het werk binnen de gemeente beter te maken. We vinden het belangrijk dat we open zijn over hoe we AI gebruiken en dat iedereen zich erbij betrokken voelt. Daarbij zorgen we er altijd voor dat de privacy en de belangen van onze inwoners voorop staan.

Strategische doelstellingen
Verbeteren van de kwaliteit en toegankelijkheid van dienstverlening
AI wordt ingezet om inwoners en bedrijven beter, sneller en toegankelijker te helpen. Denk aan verbeterde digitale dienstverlening, snellere beantwoording en betere informatievoorziening.

Verhogen van de efficiëntie van gemeentelijke processen
AI ondersteunt medewerkers door routinetaken te automatiseren, processen te stroomlijnen en werkdruk te verminderen. Dit draagt bij aan efficiëntere inzet van middelen en tijd.

Ondersteunen van datagedreven besluitvorming met menselijke controle
AI helpt bij het analyseren van gegevens en het herkennen van patronen, maar de eindverantwoordelijkheid blijft bij medewerkers. Hierdoor kunnen beslissingen beter onderbouwd worden zonder verlies van menselijke afweging.

Waarborgen van privacy, informatiebeveiliging en ethische principes
De inzet van AI gebeurt altijd met respect voor privacy, mensenrechten en ethiek. Toepassingen moeten voldoen aan wettelijke en ethische normen, inclusief transparantie, uitlegbaarheid en non-discriminatie.

Stimuleren van innovatie binnen de organisatie
De gemeente wil leren, experimenteren en innoveren met AI, binnen veilige kaders. Dit stimuleert modernisering van de organisatie en sluit aan bij ontwikkelingen binnen overheid en samenleving.

Vergroten transparantie van gegevensverwerking
AI-systemen, data en besluitvormingsprocessen worden inzichtelijk en uiteindelijk openbaar gemaakt waar mogelijk, onder andere via het algoritmeregister. Dit versterkt vertrouwen van inwoners in het gebruik van technologie.

Versterken van AI-geletterdheid en bewustwording bij medewerkers én inwoners
Om AI verantwoord in te kunnen zetten, investeert de gemeente in kennis en bewustzijn. Medewerkers krijgen ondersteuning en opleiding in het werken met AI en inwoners worden geïnformeerd over de inzet, werking en impact van AI-toepassingen binnen hun gemeente.

Typen AI-systemen

We onderscheiden drie hoofdcategorieën:

Niet-besluitvormende AI-systemen
Systemen die processen ondersteunen zonder directe gevolgen voor inwoners of bedrijven.
Voorbeelden: tekstassistenten, zoekfunctionaliteiten, interne analysetools.
Toezicht is lichter, maar voldoet aan de BIO en interne beveiligingsrichtlijnen.

- Ondersteunende systemen zonder directe besluitvormingsimpact
- Bijvoorbeeld: tekstverwerking, informatie zoeken, interne communicatie
- Beperktere controles, maar wel onder ons informatiebeveiligingsbeleid

Besluitvorming ondersteunende AI-systemen
Systemen die medewerkers helpen bij besluiten die impact hebben op inwoners, bedrijven of beleidsvorming. De uitkomst wordt altijd beoordeeld door een medewerker.
Voorbeelden: risicosignalering bij vergunningverlening, voorspelmodellen voor beleidsvorming.
Deze systemen worden geregistreerd in het algoritmeregister en vallen onder menselijke supervisie.

- Systemen die beslissingen ondersteunen met impact op inwoners, bedrijven of de gemeente
- Vereisen registratie in het algoritmeregister
- Altijd onder menselijke supervisie (Human in the loop)
- Onderworpen aan strikte controles en monitoring

Autonome AI-systemen
Systemen die zelfstandig beslissingen nemen met (mogelijke) gevolgen voor inwoners of gemeentelijke processen.
Voorbeelden: zelflerende verkeerssystemen, geautomatiseerde signaalcamera's.
Deze systemen vereisen verplichte risicobeoordelingen, fallback-mechanismen en registratie. Toepassing is alleen mogelijk waar wetgeving dit toestaat en onder strikte waarborgen.

- Systemen die zelfstandig beslissingen nemen zonder directe menselijke tussenkomst
- Kunnen impact hebben op inwoners, bedrijven of gemeentelijke processen
- Vereisen registratie in het algoritmeregister én aanvullende risicobeoordeling
- Altijd voorzien van fallback-mechanismen en periodieke evaluatie
- Voorbeelden: zelflerende verkeerssystemen, geautomatiseerde handhavingscamera's, of AI-gestuurde toewijzing van middelen

Risico's van een AI-systeem

AI-systemen brengen risico's met zich mee zoals discriminatie, gebrek aan transparantie, privacyrisico's, veiligheid, verantwoordelijkheid, manipulatie en informatiebeveiligingsrisico's (zoals modelinversie, data poisoning, DDoS en ongeautoriseerde toegang).

Deze risico's vormen de aanleiding voor:
- De voorwaarden voor AI-inzet,
- Het ethisch kader,
- De wettelijke verplichtingen,
- De AI-verordening,
- En de verplichtingen voor toezicht, audits en registratie.

De belangrijkste risico's van AI-systemen zijn:

- **Discriminatie en vooroordelen**:
  AI-modellen leren vaak van historische data. Als die data vooroordelen bevatten, kan het AI-systeem deze overnemen, wat kan leiden tot discriminerende of oneerlijke beslissingen.
- **Gebrek aan transparantie (black box)**:
  Veel AI-systemen, vooral op basis van deep learning, zijn moeilijk te doorgronden. Deep learning is een methodiek binnen AI, die is geïnspireerd door het menselijk brein en is ontworpen om patronen in data te herkennen, zoals afbeeldingen, geluid of tekst. Dit maakt het lastig om te begrijpen hoe beslissingen tot stand komen en waar fouten of vooroordelen zich kunnen voordoen.
- **Privacy risico's**:
  AI-systemen hebben vaak grote hoeveelheden data nodig, waaronder persoonsgegevens. Als in een AI-systeem persoonsgegevens worden gebruikt, kan dit leiden tot schending van privacy.
- **Veiligheid**:
  AI-systemen die ingezet worden in toepassingen zoals zelfrijdende auto's, gezondheidszorg of financiële systemen, kunnen grote schade veroorzaken als ze fouten maken of niet goed functioneren.
- **Verantwoordelijkheid**:
  Bij autonome beslissingen kan het onduidelijk zijn wie verantwoordelijk is voor fouten of schade veroorzaakt door een AI-systeem: de ontwikkelaar, de gebruiker of de leverancier?
- **Manipulatie en desinformatie**:
  AI kan worden gebruikt om desinformatie te verspreiden (bijv. deepfakes) of mensen te manipuleren, bijvoorbeeld door op maat gemaakte advertenties of content te tonen die gedrag probeert te beïnvloeden.
- **Informatiebeveiligingsrisico's**:
  Naast ethische en maatschappelijke risico's brengt het gebruik van AI-systemen ook **klassieke informatiebeveiligingsrisico's** met zich mee.
  AI-systemen kunnen kwetsbaar zijn voor:
- **Datalekken via modelinversie**: kwaadwillenden reconstrueren gevoelige informatie uit getrainde modellen.
- **Manipulatie van invoerdata (data poisoning)**: aanvallers beïnvloeden trainingsdata om de uitkomsten te vervalsen.
- **DDoS-aanvallen of systeemuitval**: waardoor AI-diensten tijdelijk niet beschikbaar zijn.
- **Onvoldoende toegangsbeveiliging**: onbevoegden kunnen modellen of data manipuleren.

Deze risico's kunnen leiden tot ongelijkheid, veiligheidsproblemen en verlies van vertrouwen in technologie. Daarom is regelgeving, zoals de AI-verordening, belangrijk om AI veilig en ethisch te ontwikkelen en in te zetten.

Voorwaarden voor AI-inzet

Dit onderdeel definieert de criteria en voorwaarden waaraan moet worden voldaan voordat AI-systemen kunnen worden ingezet. Het biedt een duidelijk beoordelingskader voor AI-initiatieven en waarborgt dat alleen passende en verantwoorde AI-toepassingen worden geïmplementeerd.

Algemene voorwaarden

- **Noodzakelijkheid en proportionaliteit**
  AI wordt alleen ingezet wanneer dit noodzakelijk is voor een publieke taak en in verhouding staat tot de impact op inwoners.
- **Wettelijke grondslag**
  De toepassing moet juridisch toegestaan zijn en voldoen aan privacy- en sectorale wetgeving.
- **Ethische verantwoording**
  AI moet bijdragen aan publieke waarde en voldoen aan de gemeentelijke ethische principes.
- **Technische haalbaarheid**
  Het systeem moet technisch betrouwbaar, uitlegbaar en uitvoerbaar zijn binnen de gemeentelijke omgeving.
- **Kosteneffectiviteit**
  De baten van AI moeten opwegen tegen de kosten voor ontwikkeling, beheer en risico's

Specifieke criteria

- Impact op privacy
- Betrouwbaarheid
- Transparantie
- Uitlegbaarheid
- Menselijke controle
- Datakwaliteit en -beschikbaarheid (in afstemming met CDO)
- Conformiteit met datastandaarden
- Data governance vereisten

Goedkeuringsprincipe
Alle AI-ondersteunde besluiten met gevolgen voor inwoners worden beoordeeld door een bevoegd medewerker.
Bij autonome AI-systemen geldt dat deze alleen worden toegestaan wanneer dit wettelijk mogelijk is, noodzakelijk is voor de taak, en wanneer realtime monitoring, fallback-mechanismen en menselijke eindverantwoordelijkheid aanwezig zijn.

Wettelijk en Ethisch Kader

Dit kader beschrijft de juridische en ethische grondslagen voor ons AI-gebruik. Het zorgt ervoor dat onze AI-toepassingen niet alleen technisch correct zijn, maar ook voldoen aan alle wettelijke vereisten en ethische normen.

Wettelijke basis

- AI Act (EU)
  Stelt verplichtingen voor risicocategorieën van AI en eisen voor transparantie, toezicht en verantwoording.
- Algemene Verordening Gegevensbescherming (AVG)
  Regelt bescherming van persoonsgegevens bij AI-gebruik.
- Europese Verdrag voor de Rechten van de Mens (EVRM)
  Waarborgt fundamentele mensenrechten zoals privacy, non-discriminatie en menselijke waardigheid.
- Wet digitale overheid
  Stelt eisen aan digitale toegankelijkheid, interoperabiliteit en betrouwbare dienstverlening.
- Data Act en Data Governance Act
  Regels over datadeling, datasoevereiniteit en gebruik van data.
- Baseline Informatiebeveiliging (BIO 2.0)
  Normenkader voor informatiebeveiliging binnen overheden.
- Wet Open Overheid (WOO)
  Verplicht transparantie en openbaarheid van AI-systemen en algoritmes.

Ethische principes
De gemeente zorgt voor een integer en non-discriminatoir gebruik van AI. Voor iedere nieuwe AI-implementatie wordt een passende beoordeling uitgevoerd. Hiermee worden mogelijke vooroordelen in

algoritmen geïdentificeerd en aangepast, zodat integere en gelijkwaardige behandeling van alle inwoners is gegarandeerd.

De gemeente hanteert zes ethische principes voor verantwoord AI-gebruik. Elk principe wordt getoetst bij de ontwikkeling, inkoop en toepassing van AI-systemen.

Principes

1. **Transparantie & uitlegbaarheid**
   AI-beslissingen moeten inzichtelijk en begrijpelijk zijn. Gebruikers en inwoners moeten kunnen begrijpen hoe de uitkomst tot stand is gekomen.
2. **Rechtvaardigheid & non-discriminatie**
   AI mag geen ongelijkheid veroorzaken of bestaande vooroordelen versterken. Bias in data en modellen moet actief worden opgespoord en verminderd.
3. **Privacy by Design**
   AI-systemen worden ontworpen met minimale gegevensverwerking en sterke bescherming van persoonsgegevens.
4. **Security by Design**
   AI-systemen worden vanaf de start voorzien van beveiligingsmaatregelen tegen aanvallen, datalekken en manipulatie.
5. **Menselijke controle**
   Menselijke beoordeling blijft altijd mogelijk. Medewerkers kunnen ingrijpen, corrigeren en beslissingen aanpassen.
6. **Maatschappelijk welzijn**
   AI-toepassingen moeten bijdragen aan publieke waarde, veiligheid en vertrouwen.

Ethisch principe	Sleutelrollen	Ondersteunende rollen
1. Transparantie & uitlegbaarheid	Proceseigenaar, FG, CDO/dataspecialist	Communicatieadviseur, SIO
2. Rechtvaardigheid & non-discriminatie	FG, CDO/dataspecialist, Privacy Officer (PO)	Proceseigenaar
3. Privacy by Design	Privacy Officer (PO), FG, CISO	CDO/dataspecialist, I&A-adviseur
4. Security by Design	CISO, I&A-adviseur	Privacy Officer (PO), CDO/dataspecialist, leveranciers
5. Menselijke controle	Proceseigenaar, FG	I&A-adviseur, SIO
6. Maatschappelijk welzijn	FG, Proceseigenaar, SIO	Communicatieadviseur, CDO/dataspecialist

Definitie van rollen:

- ***Sleutelrol*** *: primair verantwoordelijk voor beoordeling/toetsing van het principe.*
- ***Ondersteunende rol*** *: levert expertise, data, advies of technische ondersteuning.*

Verantwoordelijkheden bij ethische borging

- **Proceseigenaar**: eindverantwoordelijk voor toepassing van het ethisch kader.
- **FG/PO/CISO/CDO**: toetsen op hun expertisegebied (privacy, beveiliging, data, rechtmatigheid).
- **Ondersteunende rollen**: adviseren, leveren analyses en technische ondersteuning.
- **Governance-overleg (SIO/IB-board/Privacyboard)**: ziet toe op integrale besluitvorming en escalatie.

Compliance vereisten

Om te voldoen aan wet- en regelgeving rondom AI, hanteert de gemeente de volgende verplichte maatregelen:

- **Registratie in het algoritmeregister**
  Alle AI-systemen met impact op inwoners of besluitvorming worden geregistreerd, inclusief doel, werking, datagebruik, risico's en verantwoordelijken.
- **Uitvoering van DPIA's, IAMA's en/of DEDA's**
  Voor AI-systemen met privacy-impact, risicokarakter of maatschappelijke gevolgen worden passende beoordelingen uitgevoerd.
- **Regelmatige audits**
  AI-systemen worden periodiek gecontroleerd op werking, bias, beveiliging en correcte inzet.
- **Documentatie en verantwoording**
  Alle beslissingen, processen en aanpassingen rondom AI worden gedocumenteerd en kunnen worden verantwoord naar toezichthouders.
- **Incidentrapportage**

Incidenten met AI-systemen worden gemeld, geanalyseerd en opgevolgd volgens interne beveiligings- en privacyprocedures.

Zie ook de begrippenlijst voor meer informatie.

Compliancevereiste	Sleutelrollen	Ondersteunende rollen
Registratie in algoritmeregister	Proceseigenaar, FG	CDO/dataspecialist, I&A-adviseur, Communicatieadviseur, SIO
Uitvoering DPIA's, IAMA's en/of DEDA's	Privacy Officer (PO), FG	CDO/dataspecialist, CISO, Proceseigenaar, SIO
Regelmatige audits	CISO, FG	PO, I&A-adviseur, Interne auditfunctie, Proceseigenaar
Documentatie en verantwoording	Proceseigenaar, FG	CDO/dataspecialist, PO, I&A-adviseur, SIO
Incidentrapportage	CISO, PO	FG, I&A-adviseur, Proceseigenaar, Communicatieadviseur

Definitie van rollen:
- ***Sleutelrol*** *: primair verantwoordelijk voor beoordeling/toetsing van het principe.*
- ***Ondersteunende rol*** *: levert expertise, data, advies of technische ondersteuning.*

De AI-Verordening

De AI-verordening (AI-ACT) is een Europese wet die regels stelt voor de ontwikkeling en het gebruik van AI-systemen. Ook geeft de wet rechten aan inwoners die in aanraking komen met AI- systemen. Op 1 augustus 2024 is de AI-verordening (deels) in werking getreden. Het doel van de wet is dat AI-systemen, die door organisaties (binnen de EU) worden gebruikt, veilig zijn en fundamentele rechten respecteren. Het maakt niet uit of die AI-systemen binnen of buiten de EU zijn ontwikkeld.

Toepassingsbereik
De AI-verordening is van toepassing op:
- Aanbieders, importeurs of distributeurs van AI-systemen, of hun gemachtigde vertegenwoordigers;
- Gebruikers van AI-systemen;
- Getroffen personen van wie de gezondheid, veiligheid of grondrechten negatief wordt beïnvloed door AI-systemen.

Risicocategorieën
AI-systemen worden onderverdeeld in verschillende risicocategorieën. Afhankelijk van de categorie waarin een AI-systeem valt, gelden zwaardere, minder zware of geen regels. Deze categorisering is bedoeld om te bepalen welke reguleringsmaatregelen van toepassing zijn op verschillende AI-systemen, afhankelijk van hun potentiële impact op de samenleving en individuen.

Deze risicocategorieën zijn:
- Verboden
- Hoog-risico
- Transparantie risico (beperkt risico)

De AI-verordening gaat in fasen van kracht:

Fasering inwerkingtreding AI-verordening

Als overheidsinstantie (en potentiële gebruiker van AI-systemen) hebben we de taak om deze tijdlijn en de voorwaarden en restricties van en op AI-systemen te volgen en deze te waarborgen bij het gebruik en aanschaf van AI-systemen. Wanneer wij niet voldoen aan de AI-verordening, kunnen er verschillende maatregelen worden genomen. Deze maatregelen zijn afhankelijk van de ernst en aard van de overtreding. Toezicht wordt extern uitgevoerd door nationale toezichthouders (naar verwachting de Autoriteit Persoonsgegevens, eventueel samen met RDI). Intern zien de FG, CISO, PO en proceseigenaar toe op naleving.

Verantwoordelijkheden

Voor een succesvolle en verantwoorde implementatie van AI zijn duidelijke rollen en verantwoordelijkheden essentieel. Dit hoofdstuk beschrijft op strategisch niveau de belangrijkste rollen binnen onze AI-governance structuur. Zie ook de bijlage: *Organogram AI-Governance Gemeente Hollands Kroon*

Rol	Verantwoordelijkheden
Directie (DT)	• Eindverantwoordelijk voor besluitvorming over AI-initiatieven • Besluit op basis van advies van programma regie en AI-stuurgroep • Kan voorstellen terugsturen voor heroverweging • Toezicht op naleving van strategisch AI-beleid
Programma regie (PR) / Programma regisseurs	• Formuleert advies over de AI-adviezen die door de AI-stuurgroep worden afgegeven over AI-systemen/voorstellen (vooral bij transparantieverplichting en hoog-risico AI) • Adviseert directie over implementatie adviezen en risico's
Chief AI Officer (CAIO)	• Ontwikkelt en voert de AI-strategie uit • Voorzitter van de AI-stuurgroep • Eindverantwoordelijk voor AI-implementaties • Rapporteert aan programmaregie, directie en gemeentebestuur • Bepaalt of een systeem AI is en stelt risicocategorie vast • Stelt adviesnota's op voor programma regie
AI-Stuurgroep	• Beoordeelt AI-initiatieven • Bewaakt ethische richtlijnen (transparantie, uitlegbaarheid, non-discriminatie) • Voert/coördineert risicoanalyses (zoals DPIA's en FRIA's) • Adviseert over AI-beleid en strategische keuzes • Herziet AI-beleid periodiek • Is een samenwerking tussen CDO, FG, PO, CISO, ISO en CAIO.
Privacy Officer (PO)	• Beoordeelt AI-systemen op AVG-compliance • Voert DPIA's uit of toetst deze • Adviseert over gegevensbescherming vanaf projectstart • Waarborgt Privacy by Design • Behandelt privacy-gerelateerde klachten
Functionaris Gegevensbescherming (FG)	• Toezicht op naleving van de AVG • Onafhankelijk advies over privacyvraagstukken • Contactpersoon voor de Autoriteit Persoonsgegevens • Wordt geïnformeerd over AI initiatieven
Information Security Officer (ISO)	• Toetst op informatiebeveiliging van AI-systemen • Voert security assessments uit
Chief Information Security Officer (CISO)	• Ontwikkelt strategische beveiligingsrichtlijnen • Coördineert incident response bij AI-incidenten • Rapporteert over het gebruik van AI in het jaarverslag informatiebeveiliging. • Geeft gevraagd en ongevraagd advise rondom informatiebeveiliging.
ICT Adviseurs	• Beoordeelt technische haalbaarheid van AI-oplossingen • Zorgt voor integratie met bestaande IT-architectuur • Bewaakt technische standaarden en API's

	• Adviseert bij leveranciersselectie
Chief Data Officer (CDO)	• Ontwikkelt en implementeert datastrategie • Waarborgt datakwaliteit en governance • Beheert datastandaarden en -architectuur • Coördineert tussen databronnen en -eigenaren • Adviseert over data-aspecten van AI-projecten • Toezicht op naleving van databeleid • Stimuleert data-gedreven besluitvorming • Stem af met CAIO over data-vereisten voor AI
SIO (Strategisch Informatie Overleg)	• Het Strategisch Informatie Overleg (SIO) adviseert over AI-systemen met verhoogde risico's. • **Bij Transparantieverplichting (beperkt risico):** Het SIO beoordeelt de notitie en adviseert. Bij afwijkend advies wordt het dossier naar de directie doorgestuurd ter besluitvorming. • **Bij Hoog-risico AI-systemen:** Het SIO adviseert en stuurt het advies en de documentatie altijd door naar de directie voor formele besluitvorming. • SIO fungeert niet als nieuwe stuurgroep, maar als bestaande governance-tafel voor risico's en informatiegestuurde besluitvorming.

Binnen de gemeente moeten alle medewerkers het gebruik van AI-systemen melden bij de Chief AI Officer en\of CISO. Externe partners die AI-toepassingen inzetten, worden verplicht om dit vooraf te melden aan de gemeente. Dit proces stelt ons in staat om een actueel overzicht van AI-toepassingen te behouden en tijdig toezicht te houden op naleving.

Conclusie

Het strategisch AI-beleid van de gemeente Hollands Kroon is een belangrijke stap richting een toekomst waarin technologie en menselijke waarden hand in hand gaan. Door duidelijke richtlijnen en ethische principes vast te stellen, zorgt de gemeente ervoor dat AI op een verantwoorde en transparante manier wordt ingezet, met respect voor de privacy en rechten van haar inwoners.

Dit strategische kader vormt de basis voor verdere uitwerking in tactische en operationele procedures. Het biedt richting en houvast voor alle betrokkenen bij de ontwikkeling, implementatie en gebruik van AI-systemen binnen onze gemeente.

Met dit beleid committeren wij ons aan verantwoord gebruik van AI ten dienste van onze inwoners, onze organisatie en de samenleving als geheel.

Bijlagen

Begrippenlijst

1. **Artificiële Intelligentie (AI)**: Computersystemen die taken kunnen uitvoeren die normaal gesproken menselijke intelligentie vereisen, zoals visuele waarneming, spraakherkenning, besluitvorming en vertaling tussen talen.
2. **Machine Learning**: Een subset van AI waarbij systemen automatisch leren en verbeteren op basis van ervaring zonder expliciet geprogrammeerd te zijn.
3. **Deep Learning**: Een geavanceerde vorm van machine learning die gebruik maakt van neurale netwerken met meerdere lagen om complexe patronen in grote hoeveelheden data te herkennen.
4. **Algoritme**: Een reeks instructies of regels die door een computer worden gevolgd om een probleem op te lossen of een taak uit te voeren.
5. **Chatbot**: Een AI-aangedreven computerprogramma dat menselijke conversatie simuleert via spraak of tekst.
6. **Data Protection Impact Assessment (DPIA)**: Een proces om de privacyrisico's van een project of systeem te identificeren en te minimaliseren.
7. **FRIA**: een toetsingskader waarmee wordt beoordeeld of het gebruik van een algoritme of AI-systeem voldoet aan de principes van **Fairness, Responsibility, Inclusiveness en Accountability** binnen de publieke sector.
8. **CISO**: Chief Information Security Officer
9. **PO** : Privacy Officer
10. **FG**: Functionaris Gegevensbescherming
11. **DT**: Directie Team
12. **PR**: Programma Regie , Programma regisseurs
13. **SIO**: Strategisch Informatie Overleg, Een **SIO** is een structureel overleg binnen de gemeente waarin strategische keuzes over informatiebeheer, archivering en digitale duurzaamheid worden afgestemd tussen beleidsmakers, informatiespecialisten en archivarissen. https://zoek.officielebekendmakingen.nl/gmb-2023-291287.html

Relevante wetgeving en richtlijnen

1. AI Act (Europese Unie)

Status: Goedgekeurd op 21 mei 2024, implementatie in fasen
Doel: Reguleert de ontwikkeling en het gebruik van AI-systemen binnen de EU
Kernpunten:

- Risico-gebaseerde benadering met vier categorieën: onaanvaardbaar risico, hoog risico, beperkt risico, en minimaal risico
- Verbod op bepaalde AI-praktijken die fundamentele rechten schenden
- Strikte vereisten voor hoog-risico AI-systemen
- Transparantie-eisen voor bepaalde AI-systemen

Bron: https://artificialintelligenceact.eu/ai-act-explorer/

2. Algemene Verordening Gegevensbescherming (AVG)

Status: Van kracht sinds 25 mei 2018
Doel: Bescherming van persoonsgegevens binnen de EU
Kernpunten:

- Rechtmatigheid, behoorlijkheid en transparantie bij gegevensverwerking
- Doelbinding en minimale gegevensverwerking
- Juistheid en opslagbeperking van gegevens
- Integriteit en vertrouwelijkheid
- Verantwoordingsplicht voor de verwerkingsverantwoordelijke

3. ePrivacy Richtlijn

Status: Huidige versie van kracht, nieuwe verordening in ontwikkeling
Doel: Bescherming van privacy in elektronische communicatie
Kernpunten:

- Vertrouwelijkheid van communicatie
- Regels voor cookies en soortgelijke technologieën
- Bescherming tegen ongewenste marketing
- **4.** Artikel 10: Eerbiediging en bescherming persoonlijke levenssfeer
- Artikel 11: Onaantastbaarheid van het lichaam
- Artikel 13: Brief-, telefoon- en telegraafgeheim

5. Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv)

Status: Laatste versie van kracht sinds 2017
Doel: Reguleert de bevoegdheden van inlichtingen- en veiligheidsdiensten

Relevantie voor AI: Stelt kaders voor het gebruik van geavanceerde technologieën voor surveillance en data-analyse

6. EU Ethische Richtlijnen voor Betrouwbare AI
Status: Gepubliceerd door de Europese Commissie in 2019
Doel: Bevorderen van betrouwbare en ethische AI in Europa
Kernpunten:

- Menselijke controle en toezicht
- Technische robuustheid en veiligheid
- Privacy en data governance
- Transparantie
- Diversiteit, non-discriminatie en rechtvaardigheid
- Maatschappelijk en ecologisch welzijn
- Verantwoording

8. NL AI Coalitie Ethiek Richtlijnen
Status: Gepubliceerd en regelmatig geüpdatet
Doel: Ethische richtlijnen voor AI-ontwikkeling en -gebruik in Nederland
Kernpunten:

- Mensgerichte AI
- Betrouwbaarheid en veiligheid
- Transparantie en uitlegbaarheid
- Inclusiviteit en non-discriminatie
- Privacy en data-soevereiniteit

Tekeningen
Organogram AI-Governance Gemeente Hollands Kroon

Contactinformatie voor vragen en ondersteuning
Chief AI Officer
Team: ICT
Contact: Helpdesk@hollandskroon.nl

Nawoord
Met dit Strategische AI-beleid hebben we een belangrijke stap gezet in de toekomst van onze gemeente. Kunstmatige intelligentie is niet alleen een verzameling van slimme technologieën, maar vooral een middel om onze dienstverlening en samenwerking met inwoners en ondernemers verder te verbeteren. Het biedt kansen om efficiënter, transparanter en mensgerichter te werken.

Bij de ontwikkeling van dit beleid hebben we ons gericht op het creëren van een aanpak die past bij de behoeften en waarden van onze gemeente. Het uitgangspunt was steeds dat technologie in dienst moet staan van mensen, niet andersom. Dit blijft ook in de toekomst onze leidraad.

We zijn trots dat onze gemeente een koploper is op het gebied van innovatie. Maar we weten ook dat dit pas het begin is. AI blijft zich snel ontwikkelen, en dat betekent dat we flexibel en alert moeten blijven. Alleen samen, met open communicatie en vertrouwen, kunnen we ervoor zorgen dat AI een positieve bijdrage levert aan ons dagelijks leven.

Tot slot willen we iedereen bedanken die heeft bijgedragen aan dit beleid. Jullie ideeën, kritische vragen en betrokkenheid hebben dit document sterker gemaakt. Nu is het aan ons allemaal om deze plannen tot leven te brengen. Laten we samen bouwen aan een toekomst waarin technologie en menselijke waarden hand in hand gaan.

Dank je wel voor je betrokkenheid en inzet!