Bijlagen

Bijlage 1 - Toetsingskader Amsterdams beheerskader voor algoritmen

In dit document vindt u het door de Rekenkamer Metropool Amsterdam gebruikte toetsingskader ter beoordeling van het Amsterdamse beheerskader voor algoritmen.

1. Toetsingskader Algoritmen v1.0 (Algemene Rekenkamer), met wijzigingen van de RMA zichtbaar

Toelichting: in de eerste kolom leest u het toetsingsonderdeel (het nummer). Het originele toetsingskader bestond uit 1) onderzoeksvragen, 2) risico's, en 3) voorbeeld beheersmaatregelen. Telkens is in de eerste kolom het origineel zichtbaar, gevolgd door de aangebrachte wijziging door de Rekenkamer Metropool Amsterdam. Indien een onderdeel niet gewijzigd is, staat er 'ongewijzigd'. Indien een onderdeel geschrapt is, staat er 'geschrapt'.

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
1.01	Is het doel / zijn de doelen van het algoritme vastgesteld?	Is het doel van het algoritme vastgesteld?	Zonder eenduidigheid over het doel is geen sturing op en verantwoording over het algoritme mogelijk	Ongewijzigd	Het doel van het algoritme moet gedefinieerd worden, ook in relatie tot het maatschappelijke resultaat (outcome)	Het doel van het algoritme is gedefinieerd, ook in relatie tot de prestaties (output) en het maatschappelijke resultaat (outcome)
1.02	Vindt er op vastgelegde (periodieke) momenten een afweging plaats van de risico's over het gebruik van het algoritme?	Ongewijzigd	Zonder actueel beeld van risico's kan er geen goede afweging worden gemaakt of de voordelen van de toepassing van het algoritme opwegen tegen de nadelen	Zonder actueel beeld van risico's van het algoritme kan er geen goede afweging worden gemaakt of de voordelen van de toepassing van het algoritme opwegen tegen de nadelen	Een ingericht en gedocumenteerd proces voor risicobeheersing. Het gaat hier om het feit dat er over risico's wordt nagedacht. De beoordeling van soorten risico's en frequentie gebeurt door de auditor op basis van professional judgement	Er is een ingericht en gedocumenteerd proces voor risicobeheersing, waarbij systematisch over risico's wordt nagedacht. Risico's worden periodiek geëvalueerd door de eigenaar van het algoritme op basis van professional judgement
1.03	Beschikt de organisatie over voldoende deskundigheid, zowel kwalitatief als kwantitatief?	Ongewijzigd	Zonder voldoende deskundigheid (kwalitatief en kwantitatief) is er een groter risico op fouten	Ongewijzigd	Een beeld van de beschikbare resources (kwalitatief en kwantitatief) en sturing daarop	De benodigde interne en externe deskundigheid is in kaart gebracht (kwalitatief en kwantitatief), sturing op de inzet van de deskundigheid vindt plaats
1.04	Is het complete lifecycle management-proces rondom het algoritme gedocumenteerd?	Ongewijzigd	Een incompleet beeld op de life cycle van het algoritme bemoeilijkt sturing en beheersing	Ongewijzigd	Lifecycle management voor algoritmes of de systemen waar ze deel van uitmaken	Lifecycle management voor algoritmes of de systemen waar ze deel van uitmaken is beschreven. Bij voorkeur specifiek per algoritme, en anders generiek voor alle algoritmen
1.05	Zijn de rollen, taken, verantwoordelijkheden en bevoegdheden in het proces beschreven (inclusief eigenaarschap) en in de praktijk toegepast?	Zijn de rollen, taken, verantwoordelijkheden en bevoegdheden in het proces rondom het algoritmen beschreven (inclusief eigenaarschap)?	Onduidelijkheid over rollen, taken, verantwoordelijkheden en bevoegdheden creëert risico's	Ongewijzigd	Gedefinieerde rollen, beschreven taken, verantwoordelijkheden en bevoegdheden	De rollen, taken, verantwoordelijkheden en bevoegdheden zijn eenduidig beschreven, generiek voor alle algoritmen of specifiek voor één algoritme
1.06	Is er een overeengekomen en vastgelegde aanpak voor kwaliteits- en prestatiedoelstellingen voor algoritmes?	Ongewijzigd	Prestatiedoelstellingen en kwaliteitsdoelstellingen zijn niet meetbaar of bespreekbaar als er geen aanpak is	Ongewijzigd	Een vastgelegde aanpak voor kwaliteits- en prestatiedoelen voor algoritmes	Een vastgelegde aanpak voor het monitoren van de kwaliteits- en prestatiedoelen voor het algoritme
1.07	Zijn bij uitbesteding van onderdelen of activiteiten met betrekking tot het algoritme afspraken met betrokken externe partijen gemaakt en vastgelegd?	Ongewijzigd	Afhankelijkheid van externe deskundigen die na het ontwikkelen van het algoritme met de betreffende kennis en ervaring weggaan, waardoor continuïteit en beheersing daarna niet meer gewaarborgd is	Ongewijzigd	Vastgelegde afspraken met externe partijen, waarborgen om lock-in en te grote afhankelijkheid te voorkomen. Inclusief exit-strategie. Denk ook aan eigenaarschap van gebruikte data voor het algoritme	Ongewijzigd
1.08	Wordt het algoritme op periodieke basis gemonitord? Je kunt hierbij denken aan monitoring op beschikbaarheid, prestaties/kwaliteit, en of het algoritme voldoet aan actuele wet- en regelgeving	Ongewijzigd	Zonder monitoring is er geen beheersing mogelijk	Ongewijzigd	Ingericht proces rondom monitoring op genoemde aspecten	Ongewijzigd

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
2.01	Is het doel van het algoritme duidelijk geformuleerd en is dat geoperationaliseerd in bruikbare aspecten in het kader van de te gebruiken model en data? Welke taak of welk onderdeel van de bedrijfsvoering ondersteunt het algoritme?	Is het doel van het algoritme duidelijk geformuleerd en is dat geoperationaliseerd in bruikbare aspecten in het kader van te gebruiken model en data?	Algoritme functioneert niet in lijn met geformuleerde doelstellingen	Algoritme functioneert niet in lijn met geformuleerde doelstellingen of ondersteunt niet het beoogde onderdeel van de bedrijfsvoering	Strategische doelstelling is concreet uitgewerkt in aspecten/criteria/indicatoren	Strategische doelstelling is concreet uitgewerkt in aspecten/criteria/indicatoren en gekoppeld aan bedrijfsvoeringsprocessen
2.02A	Is er een gedeeld doel van het algoritme en is dat inzichtelijk/uitlegbaar voor eigenaar, ontwikkelaar en gebruiker?	Delen de eigenaar, ontwikkelaar en gebruiker het doel / de doelen van het algoritme?	Zonder gedeeld beeld van de doelstellingen is er een groter risico op fouten en/of verschillen in interpretatie	Ongewijzigd	Multidisciplinaire aanpak en gremia	Multidisciplinaire aanpak en gremia leggen gezamenlijke doelen vast
2.02 B	-	Is/zijn het doel / de doelen inzichtelijk en uitlegbaar voor eigenaar, ontwikkelaar en gebruiker? [NIEUW; origineel 2.02 is gesplitst in 2.02A en 2.02B].	Wanneer het doel niet uitlegbaar en inzichtelijk is, neemt de kans toe dat het algoritmen voor andere doeleinden wordt gebruikt	Ongewijzigd	Doel / doelen zijn voor een ieder toegankelijk Gemonitord wordt of het algoritme alleen voor het vooraf beoogde doel wordt toegepast	Ongewijzigd
2.03	Is het algoritme uitlegbaar en heeft er een afweging plaatsgevonden tussen de uitlegbaarheid van het model en de prestatie van het model?	Ongewijzigd	Niet of slecht uitlegbare toepassing van algoritmes beperkt de transparantie en kan tot gevolg hebben dat een bestuursrechtelijk besluit geen stand houdt	Ongewijzigd	Uitleg expliciet en indien van toepassing expliciet maken van afweging tussen uitlegbaarheid en prestaties	Ongewijzigd
2.04	Zijn de gemaakte overwegingen van het ontwerp en de implementatie vastgelegd?	Ongewijzigd	Het is niet meer te herleiden waarom welke keuzes zijn gemaakt in ontwerp en implementatie	Ongewijzigd	Vastleggen overwegingen en keuzes in ontwerp (zoals keuzes tussen modellen, ROC-curves) en tijdens implementatie. Een ROC-curve is een hulpmiddel bij beoordeling van het model	Vastleggen overwegingen en keuzes in ontwerp (zoals keuzes over welke technieken worden ingezet, welke variabelen gebruikt worden en welke assumpties gelden) en tijdens implementatie
2.05	Is er documentatie die het ontwerp en de implementatie beschrijft?	Ongewijzigd	Geen continuïteit van het proces/uitvoering van werkzaamheden doordat documentatie ontbreekt	Ongewijzigd	Actuele, complete en toegankelijke documentatie	Actuele, complete en toegankelijke documentatie; uitvoeren van peer reviews op gemaakte keuzes
~~2.06~~	Zijn de keuzes voor het gebruik van hyperparameters beargumenteerd en onderbouwd?	Geschrapt	Er heeft een willekeurige selectie van hyperparameters plaatsgevonden en daarbij zijn onjuiste keuzes gemaakt. Een hyperparameter is een parameter waarmee kan worden gestuurd op het trainings-/leerproces	Geschrapt	Uitvoeren peer review (vier-ogen-principe)	Geschrapt
2.06	Is het model (code en werking) gepubliceerd en beschikbaar voor belanghebbenden? In hoeverre zijn de gebruikte data of een beschrijving daarvan gepubliceerd en beschikbaar voor belanghebbenden?	Ongewijzigd	Ontbreken transparantie voor burgers/bedrijven/stakeholders, niet voldoen aan wet- en regelgeving met betrekking tot transparantie	Ontbreken transparantie voor burgers/bedrijven/stakeholders	Model (code) publiceren op een site zoals github.com, inclusief beschrijving van werking, gebruikte data en/of beschrijving daarvan	Model (code) publiceren op een site zoals github.com en/of een algoritmeregister, inclusief beschrijving van werking, gebruikte data en/of beschrijving daarvan
2.07	Als er sprake is van geautomatiseerde besluitvorming, wordt daarbij voldaan aan de wet- en regelgeving die daarvoor geldt?	Wordt er voldaan aan de transparantie-eis uit de AERIUS uitspraak, dat de gemaakte keuzes, gebruikte gegevens en aannames uit eigen beweging volledig, tijdig en op passende wijze openbaar moeten worden gemaakt? (Wanneer algoritmen een rol spelen bij besluitvorming.)	Gebruik van geautomatiseerde besluitvorming wanneer dat niet is toegestaan of ontbreken van de mogelijkheid van menselijke tussenkomst	Besluiten zijn onvoldoende gemotiveerd en niet transparant	Voldoen aan geldende wet- en regelgeving met betrekking tot automatische besluitvorming	In het besluit aangeven dat een algoritme een rol heeft gespeeld bij het nemen van het besluit en toelichten welke gemaakte keuzes, gebruikte gegevens en aannames het algoritme heeft gebruikt
2.08	Zijn de verschillende stakeholders/eindgebruikers van het algoritme betrokken in het ontwikkelproces?	Ongewijzigd	Te eenzijdige inbreng vergroot kans op fouten en niet voldoen aan doelen en aan wet- en regelgeving	Ongewijzigd	Betrek stakeholders/eindgebruikers met verschillende achtergronden bij ontwikkeling	Ongewijzigd

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
2.09	Welke controles zijn toegepast om de aansluiting te maken tussen de invoer en de uitvoer om zo de juistheid en volledigheid van de verwerking te garanderen?	Welke controles zijn toegepast om de aansluiting te maken tussen de invoer (data) en de uitvoer (resultaat) om zo de juistheid en volledigheid van de verwerking te garanderen?	Werking niet volgens vooraf vastgestelde opzet en werking	Ongewijzigd	Implementatie structurele controles op correcte werking	Ongewijzigd
2.10	Wordt het model periodiek geactualiseerd in lijn met actuele wet- en regelgeving?	Ongewijzigd	Model is ontwikkeld op basis van regelgeving van jaar t-1, en wordt ingezet in jaar t. De regelgeving (grenswaarden, bedragen) kan ondertussen veranderd zijn of bepaalde bepalingen zijn niet meer geldig	Ongewijzigd	Periodieke controle op voldoen aan en in lijn zijn met actuele wet- en regelgeving	Ongewijzigd
2.11	Is de kwaliteit gewaarborgd met betrekking tot keuzes die zijn gemaakt bij training- en testdata?	Hoe is de kwaliteit van de data gewaarborgd (trainings-, test- en/of validatiedata)?	Onjuiste manier van training/testing kan leiden tot overfitting en/of underfitting en/of bias	Ongewijzigd	Onder andere het aangetoond scheiden van training-, test- en validatiedata, 'vreemde ogen'/peerreview en vastlegging van proces/discussies/keuzes	Ongewijzigd
2.12	Wordt er gewaarborgd dat er geen bias wordt gecreëerd door keuzes met betrekking tot het **model**?	Ongewijzigd	Het model creëert onwenselijke systematische afwijking voor specifieke personen, groepen of andere eenheden (bias)	Ongewijzigd	Maatregelen om bias te beperken, tegen te gaan en/of te compenseren	Het model wordt periodiek getest en geëvalueerd waarbij wordt vastgesteld of het model bias bevat. Vervolgens worden maatregelen getroffen om bias te beperken, tegen te gaan en/of te compenseren
2.13	Bevat de **data** geen onwenselijke bias?	Ongewijzigd	Er zit onwenselijke systematische afwijking (bias) in de data	Ongewijzigd	Controleren/testen op bias en eventueel tegenmaatregelen nemen	Ongewijzigd
2.14	Zijn training-, test- en validatiedata gescheiden verwerkt?	Ongewijzigd	Als er niet wordt gescheiden tussen training-, test- en validatiedata, dan is er sprake van overfitting en kan het model niet gebruikt worden voor nieuwe observaties	Ongewijzigd	Zichtbaar gescheiden training-, test- en validatiedata	Ongewijzigd
2.15	Zijn de gebruikte data representatief voor de toepassing?	Ongewijzigd	De data zijn niet representatief	Ongewijzigd	Testen, controleren	Een controle waarmee wordt vastgesteld of de gebruikte data representatief zijn jegens de populatie
2.16	Heeft de (overheids)organisatie volledige controle en beheersing (eigenaarschap) over de gebruikte data voor het model?	Heeft de gemeente volledige controle en beheersing (eigenaarschap) over de gebruikte data voor het model?	Afhankelijkheid van derden met betrekking tot gebruikte data	Ongewijzigd	Voor alle databronnen/gebruikte data regelen dat er geen beperkingen/verplichtingen zijn	Ongewijzigd
2.17	Is er sprake van dataminimalisatie? Is gekeken naar proportionaliteit en subsidiariteit?	Is er sprake van dataminimalisatie, inclusief proportionaliteit en subsidiariteit?	Overtreden van geldende uitgangspunten/regels met betrekking tot dataminimalisatie en proportionaliteit	Ongewijzigd	Sturen op dataminimalisatie, expliciete afweging met betrekking tot proportionaliteit	Sturen op dataminimalisatie, expliciete afweging met betrekking tot proportionaliteit en subsidiariteit
2.18	Is de kwaliteit van het model gedocumenteerd?	Ongewijzigd	De performance metrics komen niet overeen met de doelstellingen van het algoritme	Wanneer de kwaliteit van het model onvoldoende gedocumenteerd is, is niet na te gaan en/of te verantwoorden in hoeverre de resultaten overeenkomen met de doelstellingen van het algoritme	Goede verslaglegging/audit-trail (ROC-curve)	Het documenteren van de kwaliteit van het model, eventueel aan de hand van performance metrics

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
~~2.19~~	Is er target leakage? Met andere woorden: maken de voorspellingen deel uit van de model features?	Geschrapt	De data waarop het model is gebaseerd, zijn niet beschikbaar voordat de uitkomsten zijn geobserveerd	Geschrapt	Controle op genoemd aspect (target leakage)	Geschrapt
2.19	Wordt er gebruikgemaakt van prestatie-indicatoren of performance metrics?	Hoe wordt geborgd dat de kwaliteit van de resultaten op orde is?	Kwaliteit van de voorspelling is niet op orde	Kwaliteit van de resultaten is niet op orde	Instrumenten zoals ROC-curve, confusion matrix	Gebruik van performance-metrics of prestatie-indicatoren die een beeld geven van de kwaliteit van de resultaten
2.20	Wordt de output van het model gemonitord?	Ongewijzigd	Soms werkt het model in de praktijk niet (meer)	Soms werkt het model in de praktijk niet (meer) als beoogd	Monitoren output, beoordelen en rapporteren	Ongewijzigd
2.21	Vindt er externe communicatie plaats over het model/algoritme, inclusief de beperkingen: wat kan het wel en wat niet?	Ongewijzigd	Het is voor mensen niet duidelijk dat zij met een algoritme te maken hebben, welke consequenties dat heeft of welke beperkingen het algoritme kent. Bij incidenten/fouten kan dit leiden tot schadeclaims achteraf	Het is voor mensen niet duidelijk dat zij met een algoritme te maken hebben, welke consequenties dat heeft of welke beperkingen het algoritme kent	Externe communicatie over het model/algoritme	Ongewijzigd
2.22	Vindt er onderhoud en beheer plaats op het algoritme?	Ongewijzigd	Het risico bestaat dat alle focus en effort aan de voorkant wordt gestoken in het ontwikkelen en in productie brengen van het algoritme, zonder overdracht naar degenen die het algoritme moeten beheren en ook “de business” vergeten wordt in het onderhoud	Ongewijzigd	Onderhoud en beheer op de technische componenten, het model, de gebruikte data, parameters, enzovoort	Ongewijzigd
3.01	Wordt er een register bijgehouden met betrekking tot het gebruik van persoonsgegevens?	Is het algoritme opgenomen in het verwerkingsregister indien persoonsgegevens worden verwerkt (art 30 AVG)?	Niet voldoen aan wettelijke verplichting AVG met betrekking tot bijhouden register	Niet voldoen aan wettelijke verplichting AVG met betrekking tot bijhouden verwerkingsregister	Een register bijhouden volgens AVG	Algoritme opnemen in het verwerkingsregister
3.02	Is er sprake van data protection by design?	Is er sprake van data protection by design (art 25 AVG)?	Ontwerp en opzet zijn onvoldoende gericht op bescherming van privacy	Ontwerp en opzet zijn onvoldoende gericht op bescherming van privacy, daardoor worden te veel gegevens verwerkt, te vaak verwerkt, te lang opgeslagen of zijn voor te veel personen toegankelijk	Ontwerpprincipes die privacy waarborgen	Ontwerpprincipes die privacy waarborgen Implementatie van Richtsnoeren 4/2019 inzake artikel 25 (van de European Data Protection Board; 20 oktober 2020)
3.03	Is er een DPIA uitgevoerd (indien van toepassing)?	Is er een DPIA uitgevoerd (indien van toepassing) (art 35 AVG)?	Niet voldoen aan wettelijke verplichting AVG met betrekking tot uitvoeren DPIA	Ongewijzigd	Uitvoeren DPIA	Uitvoeren DPIA; advies inwinnen van de functionaris gegevensbescherming (FG)
3.04	Is er sprake van automatische besluitvorming en zo ja: is dit toegestaan?	Is er sprake van automatische besluitvorming en zo ja: is dit toegestaan (art 22 AVG)?	Automatische besluitvorming terwijl dat volgens AVG niet is toegestaan	Automatische besluitvorming terwijl dat volgens AVG niet is toegestaan of er is niet voldaan aan de voorwaarden van de AVG	Geen automatische besluitvorming of geen documentatie (bijvoorbeeld in een Privacy Impact Assessment) waarom het is toegestaan	Ongewijzigd
~~3.05~~	Hebben de betrokkenen de mogelijkheid niet-onderworpen te zijn aan geautomatiseerde besluitvorming (indien van toepassing)?	Geschrapt	Niet voldoen aan wettelijke verplichting AVG/hanteren menselijke maat	Geschrapt	Vastgelegde en met betrokkenen gecommuniceerde procedure	Geschrapt

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
3.05	Is er sprake van data-minimalisatie?	Is er sprake van data-minimalisatie bij het verwerken van persoonsgegevens (art 5 AVG)?	Niet proportioneel gebruik/verzameling van persoonsgegevens	Niet-proportioneel gebruik / niet-proportionele verzameling van persoonsgegevens en er is geen afweging gemaakt of de doelen ook op een andere wijze kunnen worden behaald, met minder persoonsgegevens, of met persoonsgegevens die minder inbreuk maken op de privacy van de betrokkenen (subsidiariteit)	Vastlegging uitgangspunten van dataminimalisatie inclusief subsidiariteit en proportionaliteit (in werkinstructies)	Vastlegging uitgangspunten, werkinstructies
3.06	Vindt de verwerking van gegevens plaats op grond van een wettelijke taak?	Vindt de verwerking van gegevens plaats op grond van een wettelijke taak of vervulling van de taak van algemeen belang of in het kader van het uitoefenen van openbaar gezag (art 6 AVG)?	Niet-wettelijk handelen met betrekking tot verwerking van gegevens	Ongewijzigd	Vastlegging in PIA, verwerkersovereenkomst/register	Vastlegging in PIA, verwerkingsregister
3.07	Is de verwerking van (bijzondere) persoonsgegevens met het algoritme verenigbaar met het oorspronkelijke doel?	Is de verwerking van (bijzondere) persoonsgegevens met het algoritme verenigbaar met het oorspronkelijke doel (art 5 eerste lid AVG)?	Niet voldoen aan doelbinding volgens AVG	Ongewijzigd	Het is vastgesteld dat de verwerking van persoonsgegevens met het algoritme verenigbaar is met het oorspronkelijke doel (doelbinding)	Ongewijzigd
3.08	Is vastgesteld wie de verwerkingsverantwoordelijke en verwerker is van de persoonsgegevens met betrekking tot het algoritme en de daarbij gebruikte data?	Is vastgesteld wie de verwerkingsverantwoordelijke en verwerker zijn van de persoonsgegevens met betrekking tot het algoritme en de daarbij gebruikte data? (Hoofdstuk IV, afdeling 1 in samenhang met art 4 sub 7 en sub 8, AVG.)	Niet voldoen aan wettelijke verplichting AVG met betrekking tot vastlegging van verantwoordelijkheden	Niet voldoen aan wettelijke verplichting AVG met betrekking tot vastlegging van verantwoordelijkheden Niet voldoen aan de AVG als niet is onderkend dat deze verantwoordelijkheid bij de gemeente berust	De rechtmatige grondslag voor het verwerken van persoonsgegevens door het algoritme is vastgesteld	Aan de hand van de stroomschema's in de *Handleiding Algemene verordening gegevensbescherming* (min J en V, januari 2018) is vastgesteld of de gemeente een verwerkingsverantwoordelijke of een verwerker is
~~3.10~~	Is er sprake van discriminatie door gebruikte data en model?	Geschrapt	Handelen in strijd met artikel 1 uit de Grondwet (GW)/artikel 14 Europees Verdrag voor de Rechten van de Mens (EVRM)	Geschrapt	Denk aan etniciteit, huidskleur, geslacht, seksuele geaardheid maar ook postcode. Niet alleen check op data zelf is relevant maar ook zogenaamde proxies, model bias, enzovoort	Geschrapt
3.09	Is er getoetst in hoeverre er sprake is van profilering en in hoeverre dat is toegestaan?	Is er getoetst in hoeverre er sprake is van profilering en in hoeverre dat is toegestaan (art 22 in samenhang met art 4 sub 4 AVG)?	Profilering in de zin van AVG, art. 4, sub 4: risico handelen in strijd met AVG	Profilering in de zin van AVG, art. 4, sub 4, waarbij gehandeld is in strijd met art 22 AVG	Vastlegging van deze toetsing	Ongewijzigd
3.10	Is er invulling gegeven aan het proactief of op verzoek informeren van betrokkenen wier gegevens worden verwerkt/gebruikt (zowel data als algoritme)?	Is er invulling gegeven aan het proactief of op verzoek informeren van betrokkenen wiens gegevens worden verwerkt/gebruikt (zowel data als algoritme) (art 12-14 AVG)?	Niet voldoen aan wettelijke verplichting AVG met betrekking tot informeren betrokkenen	Niet voldoen aan wettelijke verplichting AVG met betrekking tot informeren betrokkenen, waarmee de gemeente richting betrokkene niet of onvoldoende transparant is	De betrokkenen worden geïnformeerd over de verwerking van persoonsgegevens door het algoritme en de verwachte gevolgen	Ongewijzigd
3.11	Zijn de logica van het gebruikte algoritme en de gebruikte gegevens voldoende duidelijk voor betrokkenen?	Indien er sprake is van een besluit, zijn de logica van het gebruikte algoritme en de gebruikte gegevens voldoende duidelijk voor betrokkenen?	Niet voldoen aan wettelijke verplichting AVG en algemene beginselen behoorlijk bestuur (abbb's) met betrekking tot logica en toegankelijkheid	Ongewijzigd	De logica, werking en gebruikte data met betrekking tot het algoritme zijn beschreven en toegankelijk	Ongewijzigd
3.12	Zijn de gevolgen van de toepassing van het gebruikte algoritme duidelijk voor betrokkenen?	Worden de gevolgen van de toepassing van het gebruikte algoritme duidelijk gemaakt voor betrokkenen?	Niet voldoen aan wettelijke verplichting AVG met betrekking tot impact op betrokkenen	Ongewijzigd	Beschrijving en onderbouwing van (mogelijkheid) tot menselijke tussenkomst bij algoritme	Ongewijzigd

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
3.13	Is er een openbaar privacybeleid waarin gebruikte data en algoritmes aan bod komen?	Is er een openbaar privacybeleid waarin gebruikte data en algoritmes aan bod komen (art 24 tweede lid AVG)?	Betrokkenen zijn niet op de hoogte van hun rechten, gebruikte algoritmes en data	Ongewijzigd	Er is een openbaar privacybeleid waarin ook gebruikte algoritmes en data aan bod komen	Ongewijzigd
4.01	Wordt loginformatie over de werking van het algoritme bewaard en toegankelijk gemaakt?	Wordt logging-informatie over de werking van het algoritme bewaard en toegankelijk gemaakt?	Zonder loginformatie is niet te achterhalen wanneer er aanpassingen zijn gedaan (audit trail)	Zonder logging-informatie is niet te achterhalen wanneer er aanpassingen zijn gedaan (audit trail)	Loginformatie wordt bewaard en is toegankelijk totdat de bewaartermijnen zijn verstreken. De bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle- en auditcyclus van de betreffende gegevens	Logging-informatie wordt bewaard en is toegankelijk totdat de bewaartermijnen zijn verstreken. De bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle- en auditcyclus van de betreffende gegevens
4.02	Wordt gecontroleerd of toegangsrechten up-to-date zijn met betrekking tot de omgeving waarin het algoritme functioneert?	Ongewijzigd	Toegangsrechten niet meer up-to-date	Toegangsrechten niet meer up-to-date, ongeautoriseerde/ onrechtmatige toegang of onbedoelde wijzigingen	Periodiek worden toegangsrechten op actualiteit getoetst en herbevestigd door het verantwoordelijke management. Zo nodig worden incidenten of wijzigingsvoorstellen ingediend	Ongewijzigd
4.03	Worden toegangsrechten aangepast zodra er een uitdiensttreding of functiewijziging van een werknemer plaatsvindt?	Ongewijzigd	Onrechtmatige toegang tot het algoritme	Ongewijzigd	Functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen	Ongewijzigd
4.04	Worden toegangsrechten uitgegeven door daarvoor bevoegde personen?	Worden toegangsrechten tot data en model uitgegeven door daarvoor bevoegde personen?	Toegang wordt uitgegeven door persoon die daarvoor niet is geautoriseerd	Toegang wordt uitgegeven door persoon die daarvoor niet is geautoriseerd met als gevolg ongeautoriseerde/onrechtmatige toegang of onbedoelde wijzigingen	Toegangsrechten worden uitgegeven aan gebruikers en beheerders na goedkeuring door een bevoegde functionaris	Ongewijzigd
4.05	Wordt functievermenging voorkomen bij de toegang van gebruikers tot het algoritme?	Wordt functievermenging voorkomen bij de toegang van gebruikers tot het algoritme en de data?	Kans op manipulatie van het algoritme bij conflicterende toegangsrechten	Kans op manipulatie van het algoritme en/of de data bij conflicterende toegangsrechten	Toegangsbeveiliging is geïmplementeerd volgens het principe 'niets mag, tenzij nodig' op alle IT-middelen	Ongewijzigd
4.06	Wordt er gebruikgemaakt van generieke beheeraccounts? Staat het aantal beheeraccounts in logische verhouding tot de beheerders?	Ongewijzigd	Hoe meer toegewezen speciale bevoegdheden, hoe meer kans op manipulatie	Hoe meer gebruikers generieke beheeraccounts toegewezen krijgen, hoe minder overzicht en hoe meer kans op fouten	Generieke beheeraccounts (root, administrator) zijn geblokkeerd of alleen te gebruiken onder registratie en toezicht	Ongewijzigd
4.07	Wordt er bij het inrichten van toegangsrechten van verschillende gebruikersgroepen/rollen gebruikgemaakt van naamgevingsconventies en systematiek?	Ongewijzigd	Gebruikersgroepen van het algoritme lastig te identificeren	Gebruikersgroepen (inclusief beheerders) van het algoritme lastig te identificeren	Voor het inrichten van toegangsrechten gelden naamgevingsconventies en een systematiek van toegangsrechten per gebruikersgroep en/of rol ter bevordering van de onderhoudbaarheid van het beheer	Voor het inrichten van toegangsrechten gelden naamgevingsconventies en een systematiek van toegangsrechten per gebruikersgroep en/of rol ter bevordering van de onderhoudsvriendelijkheid van het beheer
~~4.08~~	Worden er naamgevingsconventies gebruikt voor gebruikers en beheerders, zodat zij geïdentificeerd kunnen worden?	Geschrapt	Beheerders en gebruikers van het algoritme lastig te identificeren	Geschrapt	Voor het identificeren van gebruikers en beheerders gelden naamgevingsconventies ter bevordering van de onderhoudbaarheid van het beheer	Geschrapt
~~4.09~~	Voeren beheerders werkzaamheden als beheerder en werkzaamheden als gewone gebruiker uit onder 2 verschillende gebruikersnamen?	Geschrapt	Onduidelijkheid in wie wijzigingen/werkzaamheden aan het algoritme heeft uitgevoerd	Geschrapt	Beheerders voeren werkzaamheden als beheerder en werkzaamheden als gewone gebruiker uit onder 2 verschillende gebruikersnamen	Geschrapt
4.08	Hebben gebruikersaccounts (geen) directe toegang tot onderliggende componenten?	Ongewijzigd	Indien wel toegang tot onderliggende componenten kan manipulatie van de database plaatsvinden	Ongewijzigd	Gebruikers hebben op applicatieniveau en daarbuiten dezelfde rechten en beperkingen	Ongewijzigd

Toetsings-onderdeel	Onderzoeksvraag origineel (Algemene Rekenkamer)	Onderzoeksvraag aangepast (RMA)	Risico origineel (Algemene Rekenkamer)	Risico aangepast (RMA)	Voorbeeld beheersmaatregelen origineel (Algemene Rekenkamer)	Voorbeeld beheersmaatregelen aangepast (RMA)
4.09	Bestaat er een functiescheiding tussen aanvragen, autoriseren en verwerken van wijzigingen in gebruikersaccounts en toegangsrechten?	Ongewijzigd	Indien toegang tot onderliggende componenten kan manipulatie van de database plaatsvinden met betrekking tot functiescheiding	Ongewijzigd	Functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen	Ongewijzigd
4.10	Is het wachtwoordbeheer interactief en zijn de wachtwoorden van geschikte kwaliteit?	Is het wachtwoordbeheer interactief en zijn de wachtwoorden van geschikte kwaliteit (o.a. inhoudseisen en 2FA)?	Indien er toegang is tot onderliggende componenten kan manipulatie van de database plaatsvinden met betrekking tot wachtwoordbeheer	Ongewijzigd	Gebruikmaking van twee-factor authenticatie bij hoog-risico-zones, periodiek wijzigen van wachtwoorden, vergrendelen van accounts bij inactiviteit, en blokkeren na een vooraf ingesteld aantal foutieve inlogpogingen	Ongewijzigd
4.11	Worden wijzigingen in de code van het algoritme op een gecontroleerde wijze uitgevoerd? Denk aan het testen en accorderen/autoriseren van wijzigingen	Ongewijzigd	Ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies, niet naleven van wetgeving	Ongewijzigd	Wijzigingen worden getest en geaccordeerd. Er vindt periodieke monitoring plaats op de verwerkte wijzigingen	Ongewijzigd
4.12	Is het algoritme beveiligd, zodat er geen risico is op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies?	Is het algoritme beveiligd, zodat er verminderd risico is op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies?	Ongeautoriseerde toegang en daarmee kans op manipulatie van het algoritme (wijziging, beschadiging, dataverlies)	Ongewijzigd	Beveiliging	Cybersecurity-maatregelen zoals: • Toegangsbeveiliging • Screening personeel • Cryptografie • Fysieke beveiliging • Penetratietests • Bescherming tegen malware en ransomware
4.13	Worden er back-ups van het algoritme gemaakt en kunnen het algoritme en de data hersteld worden?	Ongewijzigd	Back-ups zijn niet in overeenstemming met het back-upbeleid. Er is geen hersteloptie bij uitval van het algoritme en er is risico van gegevensverlies	Ongewijzigd	Back-up en herstelbeleid	Back-up en herstelbeleid; Uitvoering van het back-up en herstelbeleid
4.14	Is er sprake van security by design?	Ongewijzigd	Bij het ontbreken van security by design zijn er risico's	Ongewijzigd	Security by design is gehanteerd en terug te zien als uitgangspunt. Aspecten hiervan zijn onder meer te vinden in de ISO/IEC 27000 series en verder	Security by design is gehanteerd en terug te zien als uitgangspunt. Aspecten hiervan zijn onder meer te vinden in de BIO

2. Ethiek

Toelichting: in de eerste kolom vindt u het nummer van het ethisch principe, daarna het origineel van de Algemene Rekenkamer, en in de laatste kolom het eventueel aangepaste principe door de RMA.

Nr.	Ethisch principe origineel (Algemene Rekenkamer)	Ethisch principe aangepast (RMA)
E1.1	De beslissingen die gemaakt zijn door het algoritme zijn te controleren door menselijke tussenkomst.	De beslissingen die gemaakt zijn door het algoritme zijn te controleren door menselijke tussenkomst.
E2.1	Het algoritme is veilig en doet altijd waar het voor gemaakt is.	Het algoritme is veilig en doet altijd waar het voor gemaakt is.
E2.2	Privacy is gewaarborgd en data zijn beschermd.	Privacy is gewaarborgd en data zijn beschermd.
E3.1	Het algoritme houdt rekening met diversiteit in de populatie en discrimineert niet.	Het algoritme houdt rekening met diversiteit in de populatie.
E3.2	Er is bij de ontwikkeling van het algoritme rekening gehouden met impact op maatschappij en milieu.	Er is bij de ontwikkeling van het algoritme rekening gehouden met impact op maatschappij en milieu.
E4.1	Er kan verantwoording worden afgelegd over de gevolgde procedures.	Er kan verantwoording worden afgelegd over de gevolgde procedures.
E4.2	De werking van het algoritme is te verklaren en uit te leggen.	De werking van het algoritme is verklaard en uitgelegd.

3. Normen uit de *Europese concept AI-verordening*

Toelichting: deze normen bevatten een selectie uit de normen uit de *Europese concept AI-verordening* die in onze ogen wat toevoegen aan het door ons aangepaste *Toetsingskader Algoritmen* van de Algemene Rekenkamer. Om tot deze selectie te komen, hebben we gebruikgemaakt van het voorstel van de Europese Commissie (2021), het voorlopig gezamenlijk standpunt van de Europese Raad (2022) en de door het Europees Parlement amendementen op het voorstel van de Europese Commissie (2023).

Domein	Algemene norm uit de *Europese concept AI-verordening* (i.e. wat zou het beheerskader moeten voorschrijven)	Bron norm concept EU-verordening
1. Governance, toezicht en aansprakelijkheid voor testomgeving zoals bedoeld in Titel V (alle typen AI-systemen)		
	1.0 Transparantie testen Opstellen van exitverslagen over AI-systemen die de testomgeving verlaten, en jaarverslagen m.b.t. de vooruitgang en resultaten van de uitvoering van de testomgeving, met inbegrip van goede praktijken, geleerde lessen en aanbevelingen over de opzet ervan en, waar relevant, over de toepassing van deze verordening en andere Uniewetgeving onder toezicht binnen de testomgeving.	Artikel 53 lid 5
	1.1 Transparantie testen Een korte samenvatting van het in de testomgeving ontwikkelde AI-systeem, en de doelstellingen, hypothesen en verwachte resultaten ervan worden op de website van de bevoegde autoriteiten gepubliceerd.	Artikel 54 lid 1 onder j
	1.2 Monitoring testen Inrichten van doeltreffende monitoringmechanismen om vast te stellen of zich tijdens de experimenten in de testomgeving hoge risico's kunnen voordoen voor de rechten en vrijheden van de betrokkenen wiens persoonsgegevens worden verwerkt, evenals responsmechanismen om die risico's onmiddellijk te beperken en indien nodig de verwerking stop te zetten.	Artikel 54 lid 1 onder c
	1.3 Data testomgeving De verwerking van persoonsgegevens in het kader van de testomgeving mag niet leiden tot maatregelen of besluiten die gevolgen hebben voor de betrokkenen of voor de toepassing van hun rechten inzake bescherming van persoonsgegevens.	Artikel 54 lid 1 onder f
	1.4 Data testomgeving Persoonsgegevens voor het ontwikkelen en testen van AI-systemen kunnen alleen rechtmatig worden verwerkt als deze systemen worden ontwikkeld voor het beschermen van zwaarwegend algemeen belang op een of meer van de volgende gebieden: • de openbare veiligheid en volksgezondheid, waaronder de opsporing, diagnose, preventie, beheersing en behandeling van ziekten; • een hoog niveau van bescherming en verbetering van de kwaliteit van het milieu, bescherming van de biodiversiteit, beperking van vervuiling en van de klimaatverandering en aanpassing hieraan; • de veiligheid en de veerkracht van vervoersystemen, kritieke vervoersinfrastructuur en vervoersnetwerken.	Artikel 54 lid 1 onder a
	1.5 Data testomgeving Algoritmen mogen alleen worden getest in reële omstandigheden als is voldaan aan de volgende voorwaarden: • er is een plan ingediend bij de nationale toezichthouder, en de toezichthouder heeft binnen dertig dagen geen bezwaar gemaakt; • het algoritme is geregistreerd in een EU-databank; • testen duurt niet langer dan nodig en maximaal twaalf maanden; • gebruikers en proefpersonen worden geïnformeerd; • op het testen wordt toezicht gehouden; • de voorspellingen, aanbevelingen of beslissingen van het AI-systeem kunnen worden teruggedraaid of genegeerd.	Artikel 54 bis lid 4
	1.6 Data testomgeving De testdata wordt op het juiste moment gewist en beschermd met behulp van passende technische en organisatorische maatregelen.	Artikel 54 lid 1 onder g
	1.7 Documenteren testen Een volledige en gedetailleerde beschrijving van het proces en de onderbouwing van het trainen, testen en valideren van het AI-systeem wordt samen de testresultaten bewaard als onderdeel van de technische documentatie.	Artikel 54 lid 1 onder i
2. AI-systemen met onaanvaardbaar risico		
	2.0 Periodieke toetsing Het college van B en W toetst periodiek of het AI tot de categorie onaanvaardbaar risico behoort, en motiveert waarom het AI al dan niet tot die categorie behoort.	Titel II
3. AI-systemen met hoog-risico		
	3.0 Periodieke toetsing Het college toetst periodiek of algoritmen tot de categorie AI-systemen met een hoog risico behoren op basis van de criteria in artikel 6 eerste lid en bijlage III, wanneer deze een risico vormen voor de gezondheid, veiligheid, grondrechten (en milieu).	Titel III, hoofdstuk 1
	3.1 Technische documentatie Technische documentatie wordt opgesteld voordat het AI-systeem met een hoog risico in de handel wordt gebracht of in gebruikt wordt gesteld, en wordt geactualiseerd. Met de documentatie kan worden aangetoond dat aan de verplichtingen van hoofdstuk 2 en bijlage IV is voldaan.	Artikel 11

Domein	Algemene norm uit de *Europese concept AI-verordening* (i.e. wat zou het beheerskader moeten voorschrijven)	Bron norm concept EU-verordening
	3.2 Transparantie en informatieverstrekking De werking van AI met een hoog risico is redelijkerwijs te begrijpen: gebruikers moeten in staat zijn om de output van het systeem te interpreteren en op passende wijze te gebruiken door middel van algemene kennis over hoe het AI-systeem werkt en welke gegevens het verwerkt, zodat de gebruiker de door het AI-systeem genomen beslissingen kan uitleggen aan de betrokken persoon (overeenkomstig artikel 68, punt c). AI-systemen met een hoog risico gaan vergezeld van begrijpelijke gebruiksinstructies in een passend, digitaal formaat, dat of op een andere manier beschikbaar gesteld op een duurzame drager die beknopte, juiste, duidelijke en voor zover mogelijk volledige informatie bevat die helpt bij de exploitatie en het onderhoud van het AI-systeem, die geïnformeerde besluitvorming door gebruikers ondersteunt en die redelijkerwijs relevant, toegankelijk en begrijpelijk is voor gebruikers.	Artikel 13 lid 1 tot en met 3
	3.3 Menselijk toezicht AI-systemen met een hoog risico worden zodanig ontworpen en ontwikkeld, met inbegrip van passende mens-machine-interface-instrumenten, dat hierop tijdens de periode dat het AI-systeem wordt gebruikt, op doeltreffende wijze toezicht kan worden uitgeoefend door natuurlijke personen. Het menselijk toezicht is gericht op het voorkomen of beperken van de risico's voor de gezondheid, veiligheid, grondrechten of het milieu die zich kunnen voordoen wanneer een AI-systeem met een hoog risico wordt gebruikt in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik, met name wanneer dergelijke risico's blijven bestaan ondanks de toepassing van andere voorschriften van dit hoofdstuk en wanneer uitsluitend op geautomatiseerde verwerking door AI-systemen gebaseerde besluiten rechtsgevolgen of anderszins significante gevolgen hebben voor (groepen) personen voor wie het systeem moet worden gebruikt.	Artikel 14 lid 1 en 2
	3.4 Grondrechten toetsen Beoordeling van de gevolgen voor de grondrechten van AI-systemen met een hoog risico.	Artikel 29 bis
	3.5 Verplichtingen van gebruikers Gebruikers van AI-systemen met een hoog risico gebruiken en monitoren dergelijke systemen in overeenstemming met de gebruiksaanwijzingen. De gebruiker zorgt verder (voor zover onder diens controle) voor de uitoefening van menselijk toezicht, passende maatregelen rondom robuustheid en cyberbeveiliging, relevante en representatieve inputdata, het zes maanden bewaren van de logs die automatisch worden gegenereerd en registratie in de EU-databank. Gebruikers moeten verder een gegevensbeschermingseffectbeoordeling (DPIA) en een effectbeoordeling grondrechten uitvoeren. Van beide wordt de samenvatting openbaar. Bij AI-systemen die (helpen bij) beslissingen nemen, worden de betreffende natuurlijke personen in kennis gesteld dat een AI-systeem op hen wordt toegepast.	Artikel 29
	3.6 Recht op een duidelijke en zinvolle toelichting	Artikel 68 quater
4. AI-systemen met laag of minimaal risico		
	4.0 Transparantieverplichting Het AI-systeem, de aanbieder of gebruiker moeten natuurlijke personen tijdig, duidelijk en op begrijpelijke wijze informeren dat zij interageren met systeem, uiterlijk op het eerste moment van interactie/blootstelling. Indien passend en relevant staat hier ook welke functies op AI gebaseerd zijn, er sprake is van menselijk toezicht en wie verantwoordelijk is voor het besluitvormingsproces en de mogelijkheden om in bezwaar en beroep te gaan tegen het besluit of bij schade, inclusief het recht om uitleg te krijgen.	Artikel 52
	4.1 Gedragscodes Het college van B en W stelt gedragscodes op die ertoe moeten aanzetten dat de dwingende voorschriften voor AI-systemen met een hoog-risico (zoals vastgelegd in Titel III) ook vrijwillig worden toegepast op overige algoritmes, mede om te borgen dat zij ook voldoen aan de algemene beginselen. In deze gedragscodes kunnen ook vrijwillige verbintenissen zijn opgenomen met betrekking tot bijvoorbeeld voldoende AI-geletterdheid, milieuduurzaamheid, kwetsbare groepen, gelijkheid, invloed op democratische processen, en diversiteit binnen de ontwikkelingsteams. Bij het opstellen van gedragscodes kunnen belanghebbenden worden betrokken en er moet een verantwoordelijke worden aangesteld voor de monitoring van de naleving van de gedragscodes.	Artikel 69

4. Normen uit CODIO

Toelichting: deze normen zijn overgenomen uit de Code Goed Digitaal Openbaar Bestuur (2021). In de eerste kolom leest u het nummer van de norm, in de tweede kolom het onderwerp van de norm, en in de derde kolom de norm zelf.

1. Participatie		
1.01	Burgerbetrokkenheid	De overheid betrekt burgers actief en in een open gesprek bij besluitvorming rondom en inzet van digitale middelen in bestuur.
1.02	Inclusiviteit	De overheid draagt er zorg voor dat digitale processen toegankelijk zijn voor diverse groepen in de samenleving.
1.03	Transparantie	De overheid streeft naar openheid en transparantie van zaken aangaande technologie en data en draagt er zorg voor dat (de totstandkoming van) informatie toegankelijk is voor iedereen.
1.04	Samenwerking	De overheid werkt rondom digitalisering actief samen met andere (markt)partijen, maar doet dit alleen wanneer deze derden dezelfde principes als de overheid onderschrijven.
2. Maatschappelijke waarden		
2.01	Collectieve belang	Dataverzameling en -gebruik moet ten dienste staan van collectieve belangen zoals mobiliteit, onderwijs, defensie, et cetera.
2.02	Duurzaamheid	De negatieve impact – footprint – van de inzet van digitale technologie op natuur en milieu is minimaal.

2.03	Voorkomen van schade	Bij de inzet van technologie door de overheid dient deze de veiligheid, gezondheid en het welzijn van burgers niet te schaden.
2.04	Bescherming	De overheid beschermt burgers en bedrijven tegen oneerlijke en ongewenste praktijken van (markt)partijen.
3. Mensenrechten		
3.01	Vrijheid van meningsuiting	In het gebruik van digitale systemen wordt de vrijheid van meningsuiting gerespecteerd.
3.02	Privacy	Privacy van burgers is gegarandeerd. Overheden en (markt)partijen die voor de overheid werken, gaan op prudente wijze om met persoonsgegevens (privacy-by-design principe, limiteren van verzameling persoonsgegevens, openheid richting gebruikers, et cetera).
3.03	Menselijke autonomie	De overheid of gerelateerde organisatie respecteert autonomie en zelfbeschikking van burgers, ook in relatie tot hun data.
3.04	Menselijke waardigheid	Het gebruik van digitale technologie door de overheid en samenwerkende (markt)partijen dient menselijke waardigheid (sociale samenhang, betekenisvol contact, respect, zelfontplooiing) te respecteren.
4. Procedurele rechtvaardigheid		
4.01	Passendheid	De technologie neemt de specifieke behoeftes van verschillende sociale groepen (leeftijd, cultureel, sociaaleconomisch en mensen met een beperking) in acht en zorgt indien nodig voor maatwerk.
4.02	Non-discriminatie	Gelijke kansen en gelijke behandeling zijn kernwaarden, ook bij het implementeren van digitale techniek.
4.03	Uitlegbaarheid	Uitlegbaarheid van digitale processen is cruciaal voor het vertrouwen van de burger in de overheid.
4.04	Gebruiksvriendelijkheid	De overheid zorgt ervoor dat de digitale processen goed werken voor alle verschillende gebruikers.
4.05	Aanvechtbaarheid	Overheden staan open voor klachten van burgers en burgers kunnen de beslissingen of de acties van digitale systemen van de overheid aanvechten.
4.06	Oplossingsgerichtheid	Bij problemen rondom het gebruik van technologische systemen spant de overheid zich in om oplossingen te vinden voor burgers.
5. Bestuurskwaliteit		
5.01	Wendbaarheid	De overheid werkt constant aan het updaten en verbeteren van haar digitale bestuur, streeft ernaar up to date te blijven op het gebied van innovatie en zorgt ervoor dat externe veranderingen gemakkelijk kunnen worden opgevangen.
5.02	Kennis	De organisatie borgt in de eigen organisatie kennis over hoe de technologie functioneert, en ook over de juridische en ethische eisen die hieraan worden gesteld.
5.03	Risicobewustzijn	De medewerkers zijn zich bewust [~~zijn~~] van de mogelijke impact en tekortkomingen van technologie en brengen risico's door middel van bijvoorbeeld risk assessments in kaart.
5.04	Correctie	Door middel van (peer) review, feedback en impact assessment, wordt technologie en/of haar inzet aangepast om negatieve consequenties te verhinderen en te voorkomen.
5.05	Veiligheid	De overheid zorgt ervoor dat techniek en/of digitale infrastructuur robuust en veilig voor gebruikers is en is beveiligd tegen inbraak en hackers.
5.06	Doelmatigheid	Het bestuur maakt de doelen van de digitale technologieën bekend en neemt de beslissingen en maatregelen die nodig zijn om de gestelde doelen met prudent gebruik van financiële middelen te behalen.
5.07	Onafhankelijkheid	De overheid voorkomt zoveel mogelijk dat zij voor digitale processen in hoge mate gebonden is aan één marktpartij.
6. Verantwoordelijkheid		
6.01	Aanspreekbaarheid	Uitvoerders (overheid of derden) nemen verantwoordelijkheid voor het ontwerp en onderhoud van de technologie; rollen, taken en verantwoordelijkheden zijn helder vastgelegd, en ook bij samenwerking is duidelijk wie aanspreekbaar is op gevolgen.
6.02	Verantwoording	Het bestuur legt actief aan de samenleving en politiek verantwoording af over digitaal bestuur.
6.03	Controleerbaarheid	Digitaal bestuur is transparant, begrijpelijk en open, zodat burgers en andere maatschappelijke stakeholders het werk van de overheid kunnen controleren en bijvoorbeeld inzage hebben in welke gegevens de overheid over hen heeft.
6.04	Toezicht	Overheid implementeert processen voor het geregeld plaatsvinden van interne en externe inspectie op haar digitale processen.
6.05	Integriteit	De overheid is betrouwbaar, eerlijk, oprecht en niet omkoopbaar in de aanschaf, ontwikkeling en gebruik van digitale technologie.
6.06	Menselijke eindverantwoordelijkheid	Er is altijd menselijk toezicht en menselijke eindverantwoordelijkheid voor digitale processen.