

AI en standaarden

ECP Jaarfestival 2024

side event georganiseerd door **Forum Standaardisatie**

door Willy Tadema
Rijks ICT Gilde

↓ download alvast de slides ↓





Even mijzelf introduceren:

- Willy Tadema
- AI Governance & AI Ethics consultant
- Rijks ICT Gilde
- Lid van de NEN normcommissie AI & Big Data
- Lid van het Joint Technical Committee on AI (JTC21)
- Willy.Tadema@Rijksoverheid.nl





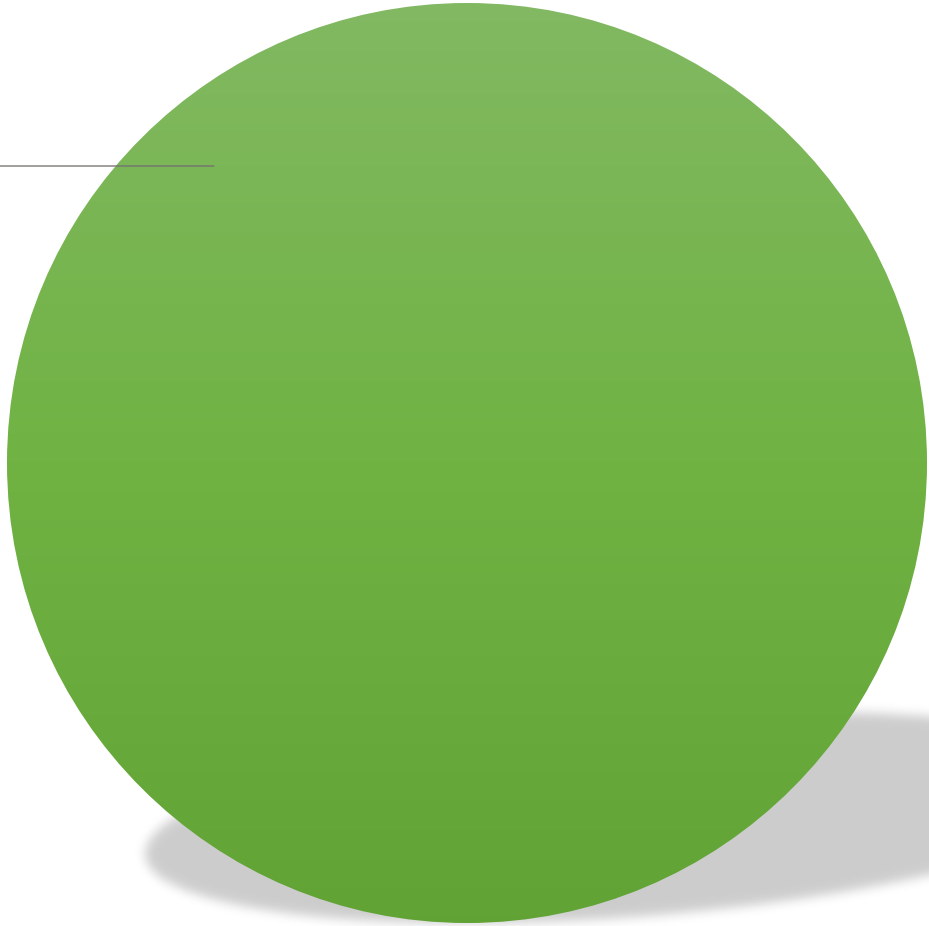
Standards

Clients

Su

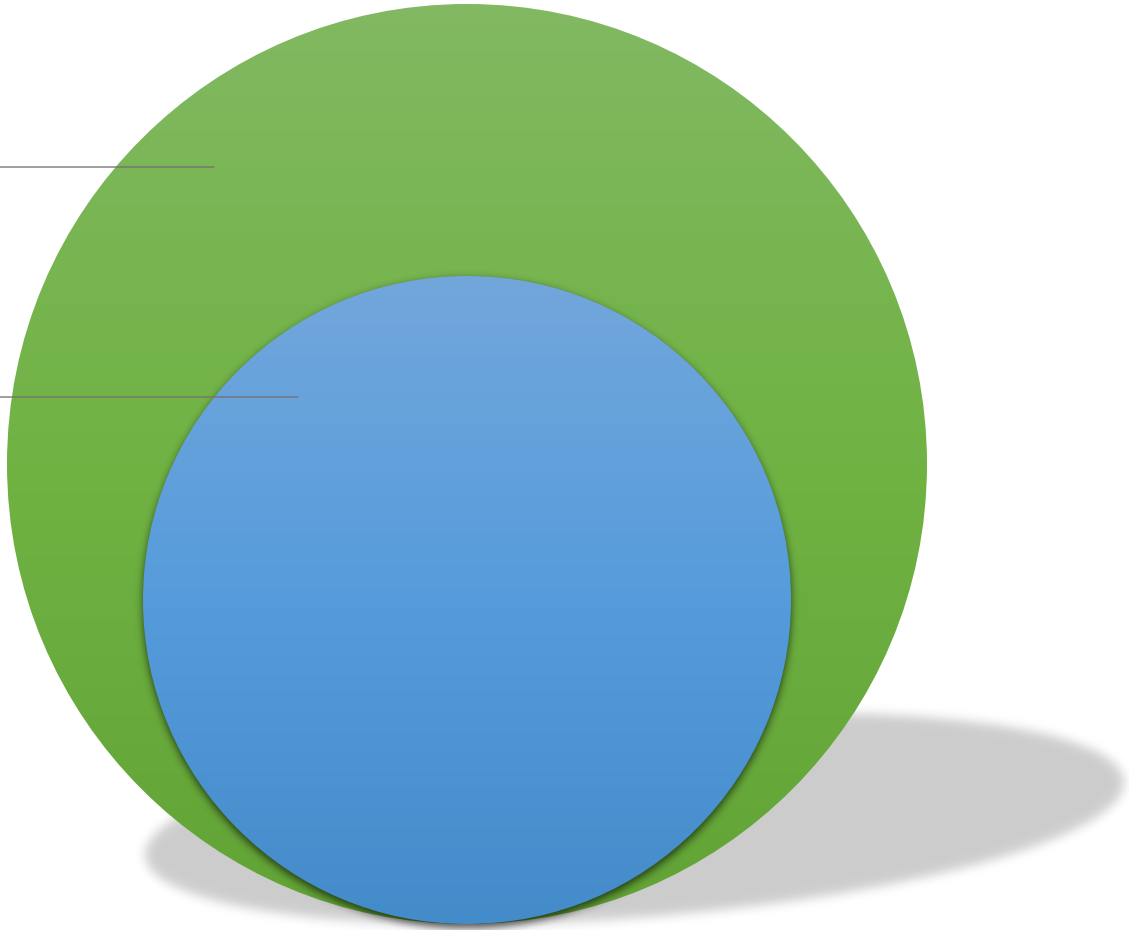
818

Standaarden



Standaarden

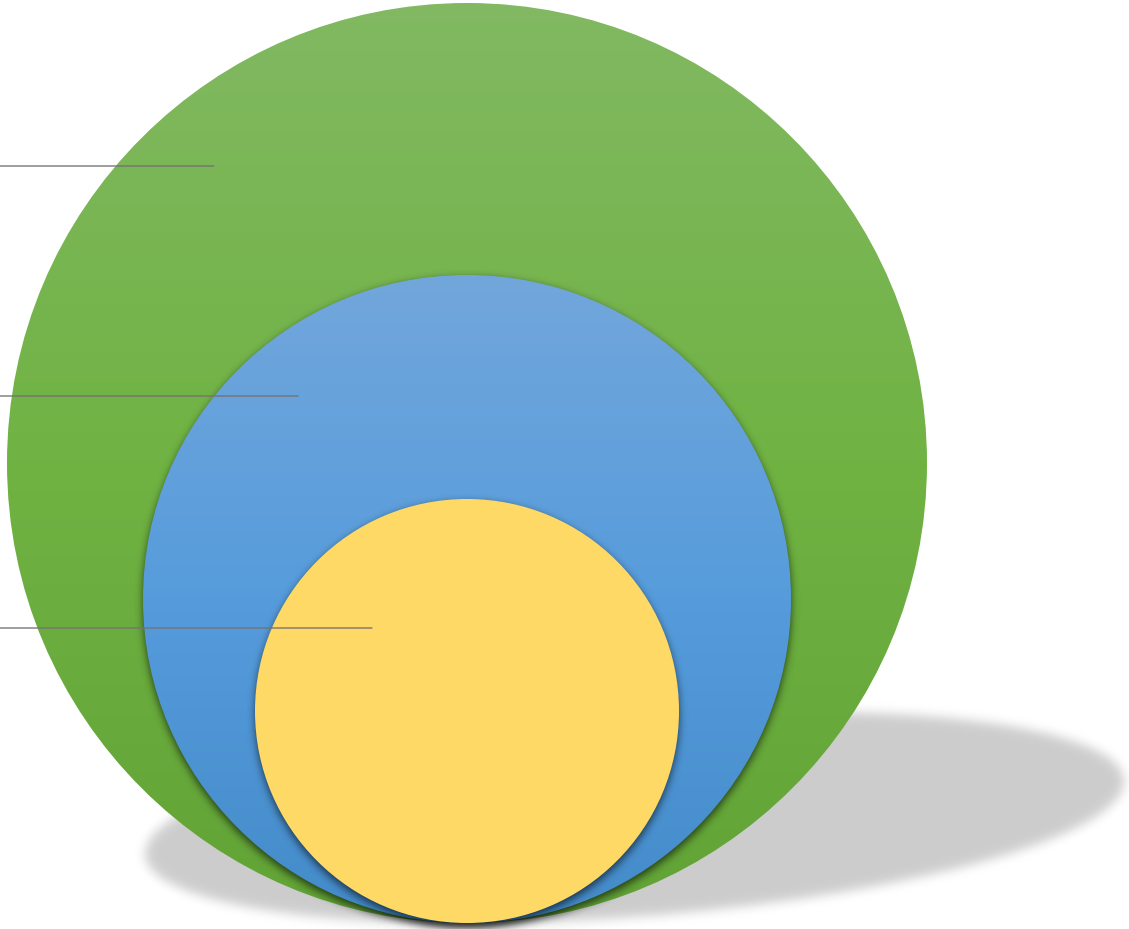
Normen



Standaarden

Normen

Europese normen (ENs)

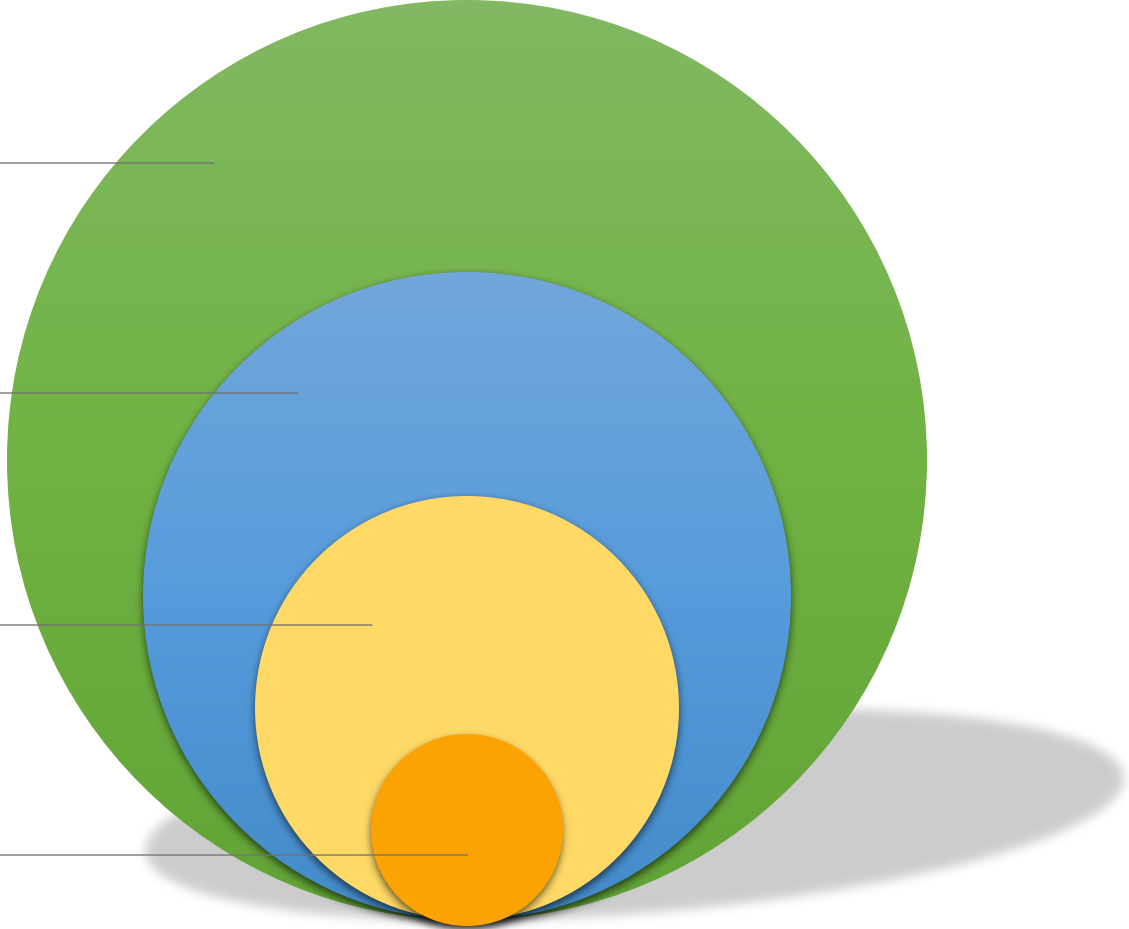


Standaarden

Normen

Europese normen (ENs)

Geharmoniseerde normen (hENs)



Wat is de **overeenkomst** tussen de **objecten in de afbeelding** en een **hoogrisico AI-systeem**?



Geharmoniseerde normen zijn een middel om compliance te beoordelen.

Het zijn technische specificaties die **meetbaar** en **testbaar**,
en daardoor **handhaafbaar** zijn.



Artikel 40

Geharmoniseerde normen en normalisatieproducten

1. AI-systemen met een hoog risico of AI-modellen voor algemene doeleinden die in overeenstemming zijn met geharmoniseerde normen of delen daarvan, waarvan de referenties in het Publicatieblad van de Europese Unie zijn bekendgemaakt, overeenkomstig Verordening (EU) nr. 1025/2012, worden geacht in overeenstemming te zijn met de in afdeling 2 van dit hoofdstuk beschreven eisen, of, naargelang het geval, de in hoofdstuk V, afdelingen 2 en 3, van deze verordening beschreven verplichtingen, voor zover die eisen of verplichtingen door die normen worden gedekt.



Judgment of the Court in Case C-588/21 P |

Public.Resource.Org and Right to Know v Commission and Others

The harmonised standards [...] form part of EU law.

[...] the Court considers that the possibility for citizens to acquaint themselves with those standards may be necessary in order to enable them to verify whether a given product or service actually complies with the requirements of such legislation.

Accordingly, the Court finds that there is an overriding public interest in disclosure of the harmonised standards in question.



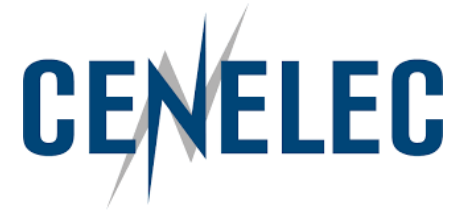
Belangrijk:

- De AI-verordening is **productwetgeving** cf. het **New Legislative Framework**.
- Een hoog risico AI-systeem heeft een **CE-markering** nodig.
Die kun je pas op het systeem 'plakken', nadat je met een **conformity assessment** hebt aangetoond dat het voldoet aan de **essentiële eisen** uit de AI-verordening.
- De meest eenvoudige manier om te voldoen aan de essentiële eisen, die ook nog juridische zekerheid biedt, is het implementeren van **geharmoniseerde standaarden**.
- Dit is dankzij de **veronderstelling van conformiteit**.



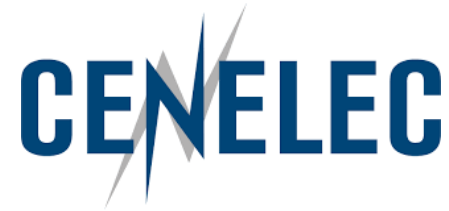


Standaardisatieverzoek (SR)



Europese standaardisatie-instituten
(ESO's)

1. De Europese Commissie (EC) publiceert een SR; ESO's accepteren het SR.



Europese standaardisatie-instituten
(ESO's)

1. De Europese Commissie (EC) publiceert een SR; ESO's accepteren het SR.
2. ESO's stellen normen op en publiceren deze als EN's.



Standaardisatieverzoek (SR)



Europese normen (EN's)



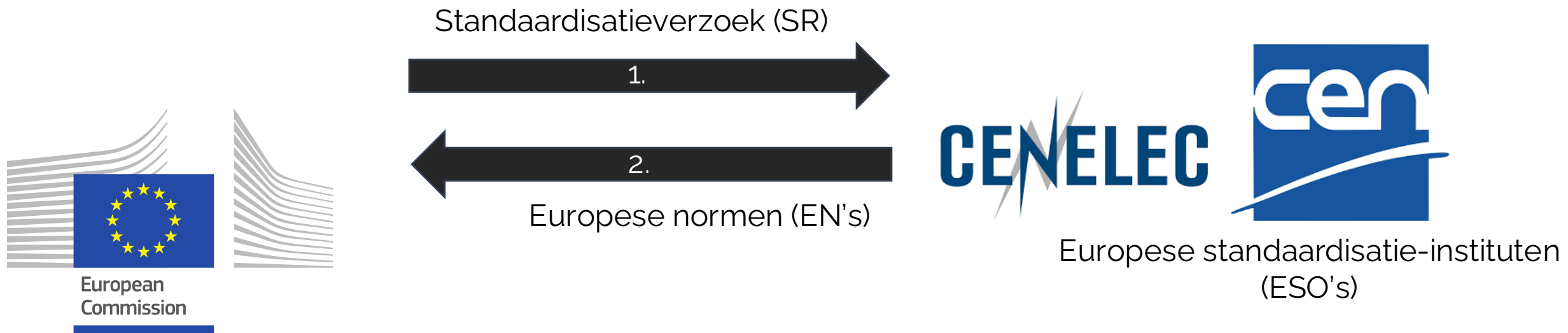
Geharmoniseerde normen (hEN's)



Official Journal
of the European Union



1. De Europese Commissie (EC) publiceert een SR; ESO's accepteren het SR.
2. ESO's stellen normen op en publiceren deze als EN's.
3. De EC toetst de EN's aan het SR, neemt ze aan en publiceert ze als hEN's.



Geharmoniseerde normen (hEN's)

3.

Official Journal
of the European Union



1. De Europese Commissie (EC) publiceert een SR; ESO's accepteren het SR.
2. ESO's stellen normen op en publiceren deze als EN's.
3. De EC toetst de EN's aan het SR, neemt ze aan en publiceert ze als hEN's.
4. Aanbieders kunnen uitgaan van het vermoeden van conformiteit.

✓ Vermoeden van conformiteit (presumption of conformity)



Standaardisatieverzoek:

1. Risk management system
2. Governance and quality of datasets
3. Record keeping through logging
4. Transparency
5. Human oversight
6. Accuracy
7. Robustness
8. Cybersecurity
9. Quality management system
10. Conformity assessment



Standaardisatieverzoek:

- | | | |
|-----------------|---|---------------------------------------|
| Art. 9 | → | 1. Risk management system |
| Art. 10 | → | 2. Governance and quality of datasets |
| Art. 11 en 12 | → | 3. Record keeping through logging |
| Art. 13 | → | 4. Transparency |
| Art. 14 | → | 5. Human oversight |
| Art. 15 | → | 6. Accuracy |
| Art. 15 | → | 7. Robustness |
| Art. 15 | → | 8. Cybersecurity |
| Art. 17, 72, 73 | → | 9. Quality management system |
| Art. 43 | → | 10. Conformity assessment |

Standaardisatieverzoek:

1. Risk management system
2. Governance and quality of datasets
3. Record keeping through logging
4. Transparency
5. Human oversight
6. Accuracy
7. Robustness
8. Cybersecurity
9. Quality management system
10. Conformity assessment

Art. 9 →

Art. 10 →

Art. 11 en 12 →

Art. 13 →

Art. 14 →

Art. 15 →

Art. 15 →

Art. 15 →

Art. 17, 72, 73 →

Art. 43 →

Deadline: 30 april 2025



New AI Act standardization requests to come early next year, EU Commission says

7 Nov 2024 | 17:14 GMT | Insight ⓘ

By [Luca Bertuzzi](#)

New standardization requests under the AI Act will be made from early next year on remote biometric identification and resource performance, including for energy efficiency of AI models, a meeting of European standardization body CEN-Cenelec's AI working group has heard. A further request from the European Commission based on the EU's code of practice for AI model providers will cover remaining obligations on model providers.

Luca Bertuzzi · Aan het volgen
Senior AI Correspondent at MLex
5 d · 🌐

The European Commission will issue new standardization requests in early 2025 under the **#AIAct** to cover biometrics and resource performance, including energy efficiency of general-purpose AI models. At a later stage, another request based on the Code of Practice will cover the rest of the requirements for GPAI models.
<https://lnkd.in/eD-bWJYP>

Vertaling weergeven

👤 144 · 7 commentaren · 19 reposts

👍 Interessant 💬 Commentaar ↻ Reposten ✈ Versturen

Voeg commentaar toe...

Relevantst ▾

Vereniging AI Advocaten (VAI-A) · 5 d ...
722 volgers
[Willy Tadema](#)
Interessant | Reageren

Baltasar Cevc · 2e (bijgewerkt) 6 u ...
Lawyer with focus on AI, ...
Good to note, thanks. The interesting question will be how long the standardization bodies will take to come up with the standards following the call. Standardization is very powerful, but coming up with ε ...meer
Vertaling weergeven
Interessant | Reageren

Vittorio Garbellotto · 3e+ · 5 d ...
Cloud Security in field service operati...
Is there any movement about creating an overall risk framework where AI, GDPR and other regulations/directives may be "put inside"? In my opinion there is too much noise, no clear directions and maybe even scopes are not well defined.
Vertaling weergeven
Interessant | Reageren



JTC21 (1)

- **CEN** en **CENELEC** hebben het standaardisatieverzoek van de EC geaccepteerd.
- De **Joint Technical Committee on AI** (JTC21) van CEN en CENELEC is met het verzoek aan de slag gegaan.
- JTC21 werkt nauw samen met nationale standaardisatieorganisaties, zoals NEN, DIN, BSI en AFNOR.
- JTC21 werkt nauw samen met de **ISO** en **IEC**, waarbij de strategie voor Europese normen t.a.v. ISO/IEC-normen is:
 1. Adopt ISO/IEC standards
 2. Adapt ISO/IEC standards
 3. Develop homegrown European standards



JTC21 (2)

- Werkgroepen:
 - WG 1 → Strategic Advisory Group (SAG)
 - WG 2 → Operational aspects
 - WG 3 → Engineering aspects
 - WG 4 → Foundational and societal aspects
 - WG 5 → Joint standardization on Cybersecurity for AI systems
- JTC21 maakt niet alleen normen, maar ook aan technische rapporten en technische specificaties.
- JTC21 maakt ook standaardisatieproducten die niet (direct) nodig zijn voor het standaardisatieverzoek.
- Het [werkprogramma](#) van JTC21 bestaat nu uit **ruim 30 standaardisatieproducten**.
- Onlangs is een snapshot van het [dashboard](#) met de voortgang in JTC21 gepubliceerd.
- Op de hoogte blijven? Abonneer je op de [AI Standardization Inclusiveness Newsletter](#).




NEN normcommissie AI & big data

- Werkgroepen:
 - WG 1 → Advisory Group
 - WG 2 → AI in de zorg
 - WG 3 → Ethiek en fundamentele rechten
- Leden van de **NEN-commissie AI & big data**:
 - bepalen gezamenlijk het Nederlandse standpunt ten aanzien van voorstellen en drafts van JTC21, waarna NL op Europees niveau (binnen JTC21) haar stem uitbrengt,
 - kunnen voorstellen doen voor nieuwe normen,
 - nemen als experts deel aan werkgroepen van JTC21 en schrijven mee aan normen,
 - vertegenwoordigen NL tijdens plenaire bijeenkomsten van JTC21.
- Leden van de normcommissie doen niet alleen mee met JTC21, maar ook met SC42.
SC42 is de subcommittee van ISO en IEC voor het ontwikkelen van mondiale AI-standaarden.

WHAT'S NEW?

De AI-verordening beschermt tegen risico's op schade aan **gezondheid** en **veiligheid**,
en een negatieve impact op de **fundamentele rechten**.



Hoe scheid je ethische en politieke vragen van technische specificaties?

Is dat eigenlijk wel mogelijk?

5.3 AI-standaarden

Europese productstandaarden zijn essentieel voor het naleven van de AI-verordening. Dergelijke standaarden bieden AI-ontwikkelaars houvast bij de vereisten uit de verordening. In het standaardisatieproces is de tijdsdruk echter hoog. Ook worden de resultaten in de vorm van productstandaarden voornamelijk niet vrij toegankelijk. Normalisatieorganisaties CEN en CENELEC ontwikkelen standaarden om nadere invulling te geven aan de eisen uit de AI-verordening. Wanneer organisaties werken volgens deze standaarden, wordt verondersteld dat hun hoogrisicosystemen voldoen aan de in de AI-verordening gestelde eisen. In de praktijk zullen de normen dus een grote rol spelen in het aantonen van compliance en de beoordeling van conformiteit.

De AP maakt zich echter zorgen over de snelheid waarmee de standaarden moeten worden opgeleverd. De normalisatieorganisaties hebben vanaf het standaardisatieverzoek van de Europese Commissie¹²⁹ slechts drie jaar de tijd voor de ontwikkeling. Doorgaans neemt het opstellen van technische productstandaarden echter veel tijd in beslag. Het opleveren van standaarden voor de AI-verordening is bovendien nog complexer, gezien de brede focus op zowel gezondheid en veiligheid als op grondrechten. Aanbieders en gebruikers van AI-systemen moet er hierdoor rekening mee houden dat de standaarden mogelijk gelijktijdig met – of pas na – de inwerkingtreding van de bepalingen over hoogrisicotoepassingen beschikbaar zijn. Beleidsmakers moeten werk maken van (het voorkomen van) een scenario waarin organisaties moeten voldoen aan de producteisen uit de verordening voordat zij de standaarden kunnen gebruiken.

Het blijft een aandachtspunt dat deze productstandaarden in beginsel enkel na betaling toegankelijk gaan worden. Vooral omdat het gaat om standaarden die moeten bijdragen aan de bescherming van grondrechten en fundamentele waarden. Doordat de normen niet algemeen toegankelijk zijn, kunnen deze minder snel doorwerken in de algemene AI-geletterdheid die organisatie- en maatschappijbreed noodzakelijk is. Het werpt ook een extra drempel op voor het algemeen publiek om controle uit te oefenen op een belangrijke uitwerking van de AI-verordening. Tegelijkertijd moet erkend worden dat het staande praktijk is dat productstandaarden – en het onderliggende standaardisatieproces – op deze manier gefinancierd worden. Als beleidsmakers ervoor kiezen om de productstandaarden publiekelijk beschikbaar te stellen, moet hier dus een passende oplossing voor gevonden worden.

Bron: Autoriteit Persoonsgegevens in de rapportage
Risico's AI en Algoritmes Nederland (RAN) van voorjaar 2024,
gepubliceerd in juli 2024.



Wat als de geharmoniseerde normen niet op tijd af zijn?

- Uitstel deadline?
- Common specifications?
- Partiële of gefaseerde geharmoniseerde normen?
- ISO/IEC-standaarden?
- Richtlijnen, bijvoorbeeld van AI Office?
- Audits door onafhankelijke 3^{de} partijen?

Hoe open zijn de geharmoniseerde standaarden?

Definitie van open standaard (IEF):

- Het proces:
 - De standaard is aangenomen en zal worden onderhouden door een non-profit organisatie.
 - De voortdurende ontwikkeling vindt plaats op basis van een open besluitvormingsprocedure die beschikbaar is voor alle geïnteresseerde partijen.
- Verspreiding van de standard:
 - De beschrijving van de standaard is vrij beschikbaar.
 - Bijbehorende patenten zijn vrij van royalty's.
 - Geen (andere) beperkingen op hergebruik.

Hoe open zijn de geharmoniseerde standaarden?

Definitie van open standaard (IEF):

- Het proces:



- De standaard is aangenomen en zal worden onderhouden door een non-profit organisatie.

?



- De voortdurende ontwikkeling vindt plaats op basis van een open besluitvormingsprocedure die beschikbaar is voor alle geïnteresseerde partijen.

- Verspreiding van de standard:



- De beschrijving van de standaard is vrij beschikbaar.

?

- Bijbehorende patenten zijn vrij van royalty's.



- Geen (andere) beperkingen op hergebruik.

Compensatie na discriminatie DUO

Publieke standaard voor profileringsalgoritmen

- Van [Algorithm Audit](#)
(ook lid van de NEN normcommissie en JTC21)
- Gebaseerd op lessons learned van Duo CUB-casus
- State-of-the-art binnen NL overheid
- Oók voor klassieke regelgebaseerde systemen, die niet onder de AI-verordening vallen
- Vrij te gebruiken en [gratis te downloaden](#)
- Kan deze standaard niet op de pas-toe-of-leg-uit lijst?

■ Zo'n tienduizend (oud-)studenten die met een discriminerend algoritme zijn gecontroleerd op fraude, krijgen geld terug van het kabinet. Minister Bruins trekt er 61 miljoen euro voor uit.

Tussen 2012 en 2023 hanteerde DUO, dat de studiebeurzen verstrekt, een fraude-selectieprocedure waarbij studenten met een migratieachtergrond eerder in beeld kwamen dan autochtone studenten. Nadat NOS op 3 en Investico daarover hadden bericht, werd de methode stopgezet.

De studenten waren beboet omdat ze ten onrechte als 'uitwonend' geregistreerd stonden en daardoor een hogere beurs kregen. Omdat het bewijs onrechtmatig is verkregen, worden zij nu gecompenseerd.

C'MON EVERYBODY!



Links:

- [Standardization Request](#)
- [JTC21](#)
- [Dashboard with JTC21 work items](#)
- [AI Standardization Inclusiveness Newsletter](#)
- [NEN-normcommissie AI en Big Data](#)
- [Harmonised Standards for the European AI Act](#) – Science for policy brief from the Joint Research Centre of the European Commission

Achtergrondinformatie:

- [The New Legislative Framework \(NLF\)](#) – Webinar CEN en CENELEC
- [The European approach to regulating through technical standards](#) – Mélanie Gornet and Winston Maxwell
- [Regulating by Standards: Current Progress and Main Challenges in the Standardization of Artificial Intelligence in Support of the AI Act](#) – Alessio Tartaro
- [Can AI standards have politics?](#) - Alicia Solow-Niederman
- [Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI](#) van Sandra Wachter e.a.
- [The fall of the great paywall for EU harmonised standards](#) – Alexandru Soroiu
- [Rapportage AI & Algoritmerisico's Nederland](#) – Autoriteit Persoonsgegevens
- [Publieke standaard voor profileringsalgoritmen](#) – Algorithm Audit



Bedankt voor je aandacht!

Meer weten over AI-normen?

Neem contact op via **Willy.Tadema@Rijksoverheid.nl** of connect via

LinkedIn **<https://www.linkedin.com/in/willytadema>**

↓ download de slides ↓

