Knowledge Centre Data & Society

Hoe voorbereiden op de AI en Data Act

KU Leuven Centre for IT and IP Law /
Kenniscentrum Data & Maatschappij
Juni 2023

Over ons

Kenniscentrum Data & Maatschappij

SMIT
Studies in Media, Innovation and Technology (VUB)

imec-mict-ugent
Research group for Media, Innovation and Communication Technologies Ghent University

KU LEUVEN CiTiP
Centre for IT & IP Law

Over ons

Kenniscentrum Data & Maatschappij

- Opgericht in 2019
- Gefinancierd door EWI
- Onderdeel Vlaams AI Plan (drie pijlers)
  1. Versterken strategisch onderzoek
  2. Stimuleren gebruikt AI in bedrijven
  3. **Bewustmaking, juridische en ethische topics**

>>Kenniscentrum Data & Maatschappij

Agenda

Kenniscentrum Data & Maatschappij

- Deep dive AI Verordening (AI Act)
  - *Presentatie*
  - *Panelgesprek*
  - *Q&A*
- Deep dive Data Act
  - *Presentatie*
  - *Panelgesprek*
  - *Q&A*
- Besluit

Knowledge Centre Data & Society

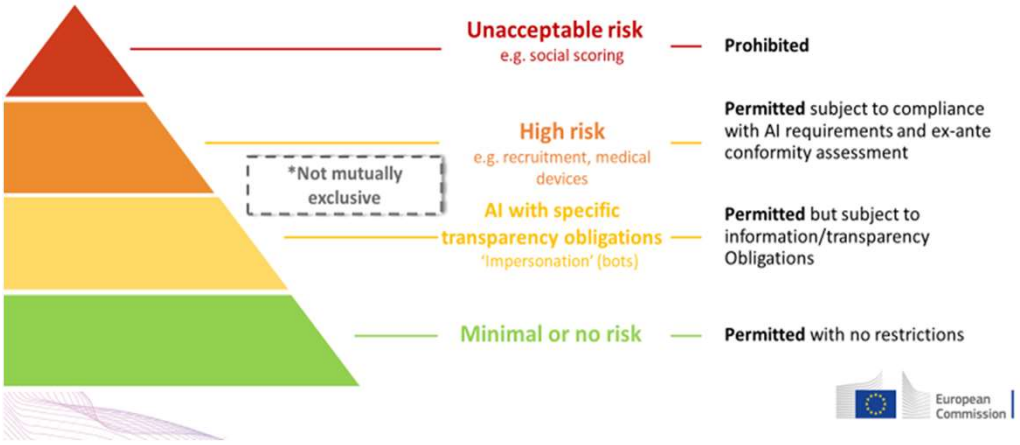
Deep Dive: AI Act

Thomas Gils
KU Leuven Centre for IT and IP Law /
Kenniscentrum Data & Maatschappij
Juni 2023

Intro AI Act

Kenniscentrum Data & Maatschappij

A risk-based approach to regulation



AI-onderzoek? (Raad)

Kenniscentrum Data & Maatschappij

- **Gebruik/ontwikkeling van AIS voor *louter* WO&O?**
  - Buiten toepassingsgebied
- **O&O naar AIS (incl. productgericht OZ)?**
  - Buiten toepassingsgebied
  - MAAR naleving erkende ethische en professionele normen

Verklaring Digitale rechten en Principes (Dec 2022)

- Hoofdstuk III: verbintenis om maatregelen te treffen die ervoor zorgen dat bij *onderzoek op het gebied van AI de hoogste ethische normen en de relevante EU-wetgeving in acht worden genomen.*

Definitie AI (EC)

Kenniscentrum Data & Maatschappij

I.	II.	III.
Software	Ontwikkeld aan de hand van **bepaalde technieken**	Die voor een bepaalde reeks door mensen gedefinieerde doelstellingen **output** kan genereren die van invloed is op de omgeving waarmee wordt geïnterageerd
	↓	
	Annex I AIA: ✓ *alle vormen van ML* ✓ *logica-gebaseerde benaderingen (incl. bv. expertsystemen)* ✓ *statistische benaderingen*	Output: *inhoud, voorspellingen, aanbevelingen of beslissingen,…*

Definitie AI (Raad)

Kenniscentrum Data & Maatschappij

I.	II.	III.	IV.
Systeem ontworpen om met een ***zekere mate van autonomie*** te functioneren	En dat, **op basis van door machines en/of mensen verstrekte gegevens en input**	aan de hand van **machinaal leren en/of logica- en kennisgebaseerde benaderingen** bepaalt hoe een bepaalde reeks door **mensen** gedefinieerde **doelstellingen** kan worden bereikt,	en door het systeem gegenereerde **output** produceert waardoor de **omgeving waarmee het AI-systeem interageert, wordt beïnvloed**
		Geen annex meer	Output: inhoud *(generatieve AI-systemen)*, voorspellingen, aanbevelingen of beslissingen

Kenniscentrum Data & Maatschappij

Hoog Risico AI-systemen

Hoog Risico AI-systemen

Kenniscentrum Data & Maatschappij

AI-systeem = hoog risico in **2 gevallen:**

- AIS = (onderdeel van bepaald) product → conformiteitsbeoordeling
- AIS met toepassing in bepaalde sector + doeleinde

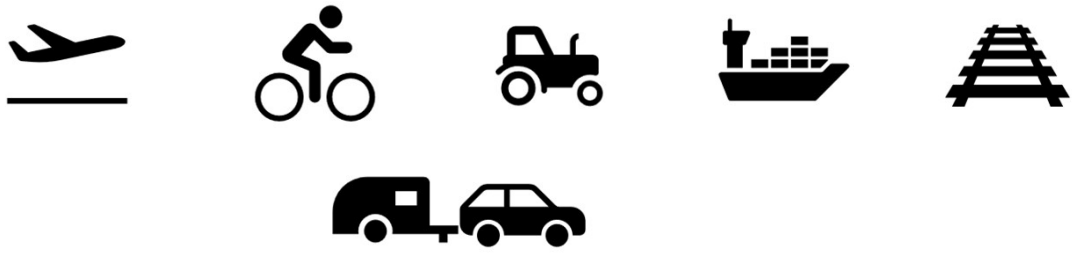
Type 1 Hoog Risico

Kenniscentrum Data & Maatschappij

AI = hoog risico indien:

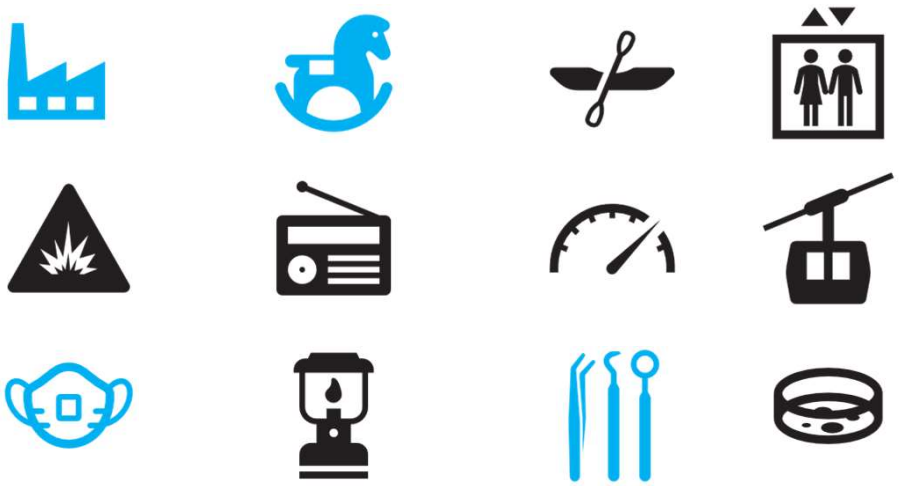
- AIS = **product of VC v/e product** dat onder deel A van de lijst van wetgeving in Annex II valt
- **EN** dit product vereist conformiteitsbeoordeling door 3e partij

Welke producten niet? (= Deel B van Annex II)



Welke producten wel?

Kenniscentrum Data & Maatschappij



Type 2 Hoog Risico (EC/Raad)

Kenniscentrum Data & Maatschappij

- **Biometrische identificatie en categorisering van natuurlijke personen**
  - Op afstand van natuurlijke personen in real time en achteraf
- **Beheer en exploitatie van kritieke infrastructuur:**
  - VC bij beheer of exploitatie van wegverkeer en de levering van water, gas, verwarming en elektriciteit
- **Onderwijs en beroepsopleiding:**
  - Bepaling van toegang tot of de toewijzing aan onderwijsinstellingen
  - Beoordeling van studenten en deelnemers
- **Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid:**
  - Aanwerving of selectie van kandidaten (incl. screenen of filteren van sollicitaties, de evaluatie van kandidaten)
  - Beslissingen over de bevordering en beëindiging van arbeidsrelaties, voor de toewijzing van taken en voor het toezicht/evaluatie van arbeidsprestaties

Type 2 Hoog Risico (2)

Kenniscentrum Data & Maatschappij

- **Toegang tot en gebruik van essentiële particuliere diensten en openbare diensten en uitkeringen**:
  - Gebruik door of namens overheidsinstanties om te beoordelen of burgers in aanmerking komen voor overheidsuitkeringen en –diensten (incl. intrekken etc.)
  - Beoordeling van kredietwaardigheid van natuurlijke personen
  - Gebruik voor de inzet of voor het vaststellen van prioriteiten bij de inzet van hulpdiensten
  - Risicobeoordeling en prijszetting bij levens- en gezondheidsverzekeringen
- **Rechtshandhaving** *(beperkt tot rechtshandhavingsautoriteiten)*:
  - Gebruik voor het uitvoeren van individuele risicobeoordelingen van natuurlijke personen om te beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit pleegt of hoe groot het risico is voor mogelijke slachtoffers van strafbare feiten;
  - Leugendetectoren of soortgelijke hulpmiddelen ter vaststelling van de emotionele toestand van een natuurlijke persoon;
  - [Gebruik voor de opsporing van deep fakes]
  - Gebruik voor de beoordeling van de betrouwbaarheid van bewijsmateriaal
  - Gebruik voor het voorspellen van een daadwerkelijk of potentieel strafbaar feit dat (opnieuw) zal worden gepleegd, op basis van de profilering van natuurlijke personen of de beoordeling van persoonlijkheidskenmerken en kenmerken of eerder crimineel gedrag van natuurlijke personen of groepen;
  - Gebruik voor de profilering van natuurlijke personen tijdens de opsporing, het onderzoek of vervolging van strafbare feiten; […]

Type 2 Hoog Risico (3)

Kenniscentrum Data & Maatschappij

- **Migratie, asiel en beheer van grenscontroles** *(beperkt tot door bevoegde overheidsinstanties):*
  - Leugendetectoren of soortgelijke hulpmiddelen voor de vaststelling van de emotionele toestand van een natuurlijke persoon;
  - Gebruik voor de beoordeling van een risico, waaronder een beveiligingsrisico, een risico op illegale immigratie of een gezondheidsrisico, dat een natuurlijke persoon vormt die voornemens is het grondgebied van een lidstaat te betreden of dat heeft gedaan;
  - [Gebruik voor de verificatie van de authenticiteit van reisdocumenten en ondersteunende documentatie van natuurlijke personen en de opsporing van niet-authentieke documenten door de controle van hun beveiligingskenmerken;]
  - Ondersteunen bij het onderzoek van asielaanvragen, aanvragen voor een visum en aanvragen voor een verblijfsvergunning, evenals gerelateerde klachten met betrekking tot de geschiktheid van de natuurlijke personen die een aanvraag voor een status indienen;
- **Rechtsbedeling en democratische processen:**
  - Ondersteuning van rechterlijke instanties bij het onderzoeken en uitleggen van feiten en de wet en bij de toepassing van het recht op een concrete reeks feiten.

Kenniscentrum Data & Maatschappij

Vereisten & verplichtingen?

Vereisten en verplichtingen

Kenniscentrum Data & Maatschappij

Systeem voor risicobeheer

- Periodieke risicoanalyse
- Gehele levensduur AIS
- Maatregelen
- Testing

Data en databeheer

- Passende gegevensbeheerspraktijken
- Gegevenskwaliteitsvereisten (*relevant, representatief, en in de mate vh mogelijke foutenvrij en volledig*)

Technische documentatie

- Doel: *controle faciliteren*
- Details in Annex IV (*ontwikkelingsproces, relevantie parameters, testprocedures,…*)

Registratie

- Doel: *Traceerbaarheid werking AIS (EC)*
- Automatische registratie van events: "logging"
- Minimumvereisten voor biometrische identificatie

Vereisten en verplichtingen (2)

Kenniscentrum Data & Maatschappij

Transparantie en informatieverstrekking aan gebruikers

- Doel: *gebruikers in staat te stellen (de output van) het systeem te begrijpen en op passende wijze te gebruiken*
- Gebruiksaanwijzingen (met minimuminformatie)
  - *o.a. beoogd doeleinde, 'specificaties voor inputdata', mate van nauwkeurigheid,…*

Menselijk toezicht

- Doel: *doeltreffend menselijk toezicht toelaten*
- Ingebouwd ofwel door de gebruiker zelf
- Minimumvereisten:
  - *Werking monitoren*
  - *Automation bias*
  - *Output v AIS negeren of ongedaan maken*
  - **…**

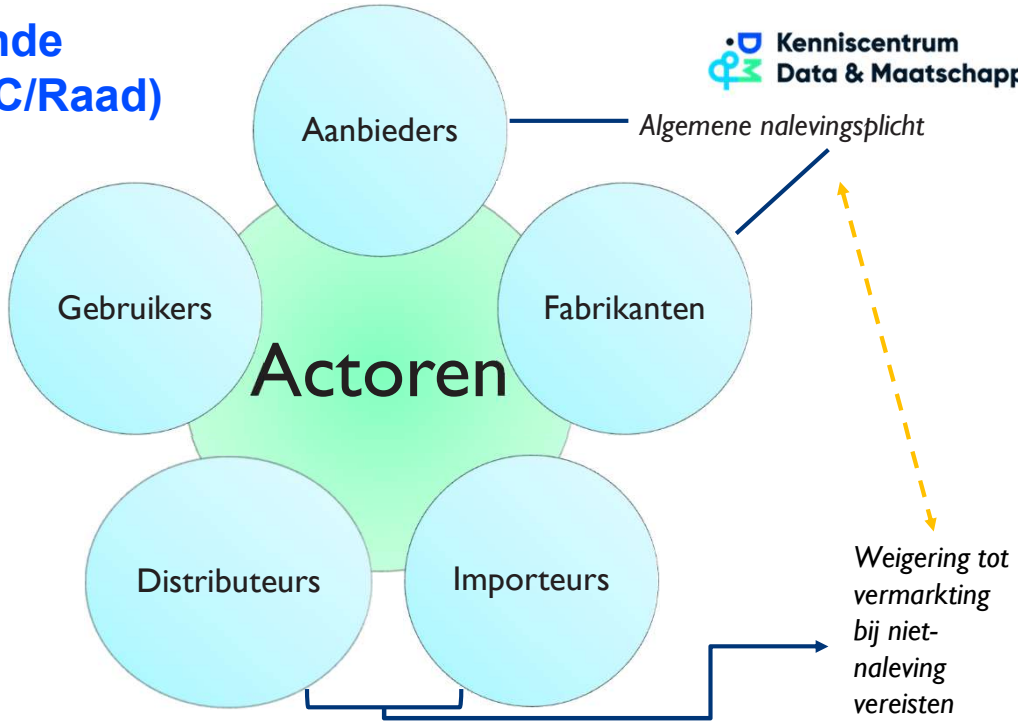
Nauwkeurigheid, robuustheid en cyberbeveiliging

- **Nauwkeurigheid**: vermeld in GA
- **Robuustheid**: o.a. feedback loops beperken
- **Cyberbeveiliging**: o.a. tegen data poisoning en adversarial examples

Kenniscentrum Data & Maatschappij

Rollen en verantwoordelijkheden?

Verschillende actoren (EC/Raad)



Aanbieders	Fabrikanten	Importeurs	Distributeurs	Gebruikers
Algemene nalevingsplicht	Algemene nalevingsplicht *(producten Annex II – Deel A + onder naam van F)*	Technische documentatie	CE-markering (+ GA)	Informatieplicht tav A & D autoriteiten *(bep. risico's + incidenten)*
Kwaliteitsbeheer *(prop. tav grootte organisatie)*		Conformiteitsbeoordeling	Informatieplicht tav A,I & autoriteiten *(bep. risico's)*	Retentie logs (mits controle)
(Technische) documentatie		CE-markering (+ GA)	Samenwerkingsplicht m. autoriteiten	Samenwerkingsplicht m. autoriteiten
Retentie logs (mits controle)		Informatieplicht tav A & autoriteiten *(bep. risico's)*	Corrigerende maatregelen *(of door A/I) (⇔ definitie?)*	
Conformiteitsbeoordeling		Samenwerkingsplicht m. autoriteiten		
CE-markering		***Specifieke vpln***		
Corrigerende maatregelen *(info → D&I)*		Naam- en adresvermelding *(Raad: ook aanbieders)*	Gepaste opslag- en vervoersomstandigheden	Gebruik, menselijk toezicht & monitoring v werking // aanwijzingen
Informatieplicht tav autoriteiten *(bep. risico's)*		Gepaste opslag- en vervoersomstandigheden		Relevante inputdata (mits controle)
Registratie in HR DB				GEB (indien relevant)
Samenwerkingsplicht m. autoriteiten		*Weigering tot vermarkting bij niet-naleving vereisten*		Raad: Registratie in HR DB *(indien overheden)*

Overzicht van (mogelijke) documenten

Kenniscentrum Data & Maatschappij

- Risicobeheerbeleid (incl. testbeleid ifv accuraatheid, robuustheid en cyberveiligheid?)
- Gegevens(beheer)beleid- en procedures
- Technische documentatie (Annex IV)
- Gebruiksaanwijzingen (incl. toezichtsmaatregelen voor gebruiker)
- **Kwaliteitsbeheerprocedure** (art. 17):
  - *Nalevingstrategie*
  - *Procedures mbt ontwerp, ontwikkeling, kwaliteitscontrole, test en validatie van AIS*
  - *Technische specificaties (incl. standaarden)*
  - *Post market monitoring-documenten (incl. PMMP – template EC)*
  - *Incident procedure + communicatieplan (tav autoriteiten e.d.)*
  - *Documentbeheer*
  - *Interne verantwoordelijkheidsverdeling*
- Documenten gerelateerd aan conformiteitsbeoordeling (o.a. conformiteitsverklaring (art. 48 & Annex V), certificaat aangemelde instantie (Annex VII)
- Documenten gerelateerd aan registratie in Hoog Risico database (Annex VIII)

Art. 28 AIA: Wijziging van hoedanigheid

Kenniscentrum Data & Maatschappij

- Importeur/distributeur/gebruiker/derde ➔ aanbieder, indien:
  1. *Vermarkting (bestaand) HR AIS onder eigen (merk)naam*
  2. *Wijziging beoogde doel*
  3. *Ingrijpende wijziging HR AIS*
  4. *Raad: vermarkting GPAI als HR AIS*

- **EC:**
  - **Geval 1**: Gezamenlijke verantwoordelijkheid?
  - **Geval 2 en 3**: Initiële aanbieder ≠ aanbieder
- **Raad:**
  - **Geval 1 en 3**: Initiële aanbieder ≠ aanbieder
  - **Geval 2 en 4**: Gezamenlijke verantwoordelijkheid?

Kenniscentrum Data & Maatschappij

AI met specifieke transparantieverplichtingen

Art. 52

Kenniscentrum Data & Maatschappij

- **Interactieve AI-systemen**
  - *Op de hoogte brengen v. artificiële interactie tenzij duidelijk*
- **Biometrische categorisatie & emotieherkening**
  - *Op de hoogte brengen van blootstelling en werking*
- **Deep fakes**
  - *Op de hoogte brengen v. artificiële aard van content, tenzij bv. onderdeel artistiek werk.*

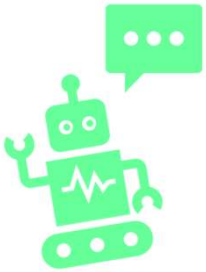
Verplichtingen op gebruikers van GPAI/FM?

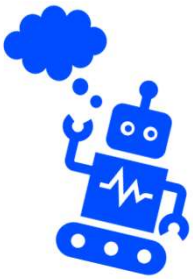
Kenniscentrum Data & Maatschappij

- **Raad**
  - Specifieke vpln op aanbieders van *General Purpose AI-systemen* (mits HR-gebruik)
  - 'ongeacht *fine-tuning* (?) door gebruikers'
  - Gebruikers: vpln zie eerder
- **Parlement**
  - Specifieke vpln op aanbieders van '*Foundational Models*'
  - Specifieke vpl mbt transparantie rond trainingsgegevens

Kenniscentrum Data & Maatschappij

Panelgesprek/Q&A





thomas.gils@kuleuven.be

Knowledge Centre Data & Society

Deep Dive: Data Act

Wannes Ooms
KU Leuven Centre for IT and IP Law /
Kenniscentrum Data & Maatschappij
juni 2023

Dataverordening (Voorstel EC)

Kenniscentrum Data & Maatschappij

- **Doel**: (IoT-)data beschikbaar tvv gebruiker/andere bedrijven/overheid
  → meer data gedreven innovatie

B2C & B2B IoT Gegevensdeling	FRAND beschikbaarheid van gegevens	Oneerlijke bedingen gegevenstoegang en -gebruik
B2G Gegevensdeling *(uitzonderlijke noodzaak)*	Cloud Switching	Interoperabiliteit van DS & DPS

Documenten	Overeenkomsten	Procedures	Technische maatregelen
Informatieplicht IoT fabrikant of dienstverlener	Overeenkomst **datadeling** IoT producten: Voorwaarden voor deling met gebruiker of derde	Verplichte datadeling met **overheid** voor uitzonderlijke noodzaak	Beschikbaar maken data aan gebruiker IoT product
Verantwoording gevraagde **vergoeding** • Wettelijk verplichte beschikbaarheid • Verplichte deling met overheid voor preventie, herstel of algemeen belang	Standaardcontracten: • Vermijden **oneerlijke bedingen** • Respecteren verplichtingen Data Act		**Technische beschermingsmaatregel** voor gedeelde data
	Dataverwerkingsdiensten wegnemen belemmeringen		Interoperabiliteitsvereisten

Documenten

Kenniscentrum Data & Maatschappij

- **Informatieplicht** IoT fabrikant of dienstverlener
  - Voor contractsluiting
  - Aard & volume, frequentie, toegangswijze, eigen of derde gebruik
  - Identiteit en contactgegevens datahouder, deling met derden, klachtenrecht
- Aantonen **redelijkheid vergoeding** voor wettelijk beschikbaar maken data
  - Redelijke vergoeding (µ- en KMO's: ≤ vergoeding kosten)
  - Voldoende gedetailleerde informatie over de berekening
- Aantonen **redelijkheid vergoeding** voor B2G datadeling
  - Vergoeding ≤ kosten verzoek (incl. anonimisering en technische aanpassing), + redelijke marge

Overeenkomsten

Kenniscentrum Data & Maatschappij

- **Bescherming bedrijfsgeheimen** bij IoT-datadeling
  - Specifiek noodzakelijke maatregelen tov gebruiker of derde
  - Vertrouwelijkheid bedrijfsgeheim waarborgen
  - Derde: specificatie bedrijfsgeheim en maatregelen
- **Oneerlijke bedingen** standaardcontracten
  - Eenzijdig => µ- & KMO's
  - Controle **zwarte en grijze lijst**
    - Beperking aansprakelijkheid opzet of grove nalatigheid, uitsluiting rechtsmiddelen/aansprakelijkheid niet-nakoming of exclusief recht overeenstemming van data te bepalen
    - Rechtsmiddelen ongepast beperken, toegang data met aanzienlijke schade belangen, hinder gebruik aangeleverde data, hinder kopieren data tijdens looptijd of onredelijke opzegtermijn
  - Controle algemene norm

Overeenkomsten (2)

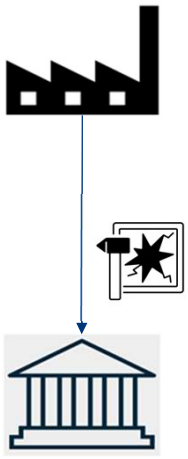
Kenniscentrum Data & Maatschappij

- Aanbieders **dataverwerkingsdiensten** (cloud providers)
  - Verwijderen contractuele belemmeringen
    - Opzegtermijn max. 30 kalenderdagen
    - Exclusiviteitsovereenkomsten
    - Functionele gelijkwaardigheid
  - Contractvoorwaarden
    - Maximale overgangsperiode 30 kalenderdagen met ondersteuning
    - Specificatie en minimum exporteerbare categorieen
    - Minimumtermijn opvragen data

Procedure

Kenniscentrum Data & Maatschappij

- **Overheidsverzoek** bij uitzonderlijke noodzaak
  - Terbeschikkingstelling data
  - Afwijzen verzoek of vraag wijziging
  - Binnen 5 of 15 werkdagen
  - Verantwoording afwijzing of wijzigingsvraag



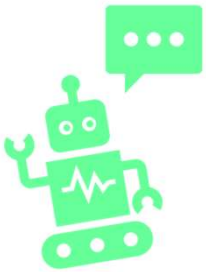
Technische maatregelen

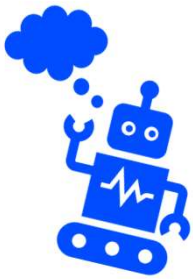
Kenniscentrum Data & Maatschappij

- Maatregelen voor deling IoT data
  - Ontwerp voor **toegankelijkheid** data
  - Toegang op eenvoudig elektronisch verzoek
- **Beschermingsmaatregelen** (bv. slimme contracten)
  - Voorkomen ongeoorloofde toegang
  - Naleving regels derdedeling en overeenkomsten
- Interoperabiliteitvereisten
  - Exploitanten dataruimten
  - Dataverwerkingsdiensten
  - Gebruiker slimme contracten

Kenniscentrum Data & Maatschappij

Panelgesprek/Q&A

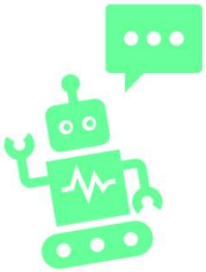




wannes.ooms@kuleuven.be

Kenniscentrum Data & Maatschappij

Bedankt



Contact
data-en-maatschappij.ai/

thomas.gils@kuleuven.be
wannes.ooms@kuleuven.be
jan.debruyne@kuleuven.be