“ By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it. ,,

Eliezer Shlomo Yudkowsky

Machine Intelligence
Research Institute (MIRI)

XYNA.AI

AI beyond
the mainstream

Philipp Dominitzki &
Dr. Kai Schorstein

OpenRheinMain 2023
Darmstadt, 2023-09-22

h_da
DARMSTADT UNIVERSITY
OF APPLIED SCIENCES

XYNA.AI

- **New business unit for AI solutions** (since 2022)
- AI consultancy, AI PaaS, GenAI language solutions (bots)
- Linked to process automation in complex environments

XYNA.COM

- **Xyna Factory:** our homebase and origin (since 2004)
- Platform for process automation with graphically modeled workflows: event-driven + order-oriented
- Cloud- & container-ready, high-load capable and scalable for tier-1 operations
- Open Source on GitHub + commercial editions with service & support options

gip

thinking beyond computing

- **Xyna.AI is part of the GIP group**
- Smart Solutions for a Connected World
- System integrator for Telco OSS solutions (since 1998)
  - Service provisioning (access, L2/L3 VPN, carrier services, …)
  - SD-x solutions (incl. order management, roll-out automation, …)
  - Network activation & abstraction (CPE, PE, DNS, DHCP, …)

- Customers: Tier-1 Telco Provider
- Reference: Deutsche Telekom
  - Frame contract for xyna.com
  - Various network automation platforms based on Xyna Factory

Philipp Dominitzki

Dipl.-Kaufmann, Master of Laws (LL.M.)

- Chief Operations Officer @ GIP Exyr GmbH
- Official representative @ Xyna GmbH

- 20y in IT & Telco
- Responsible for a team of ~ 60 consultants and IT experts

- Academic background in business informatics and IT law
- 25y in German Informatics Society

Dr. Kai Schorstein

Dipl.-Physiker

- Research Fellow @ GIP Research Institute
- Senior Consultant @ GIP Exyr GmbH
- AI Solution Engineer @ Xyna GmbH

- Member of the Xyna Innovation Board [XIB]
- Focus on architecture + specification

AI beyond the mainstream

AI & Network Automation

AI and autonomous networks empowering the next digital transformation

the European AI Act (AIA)

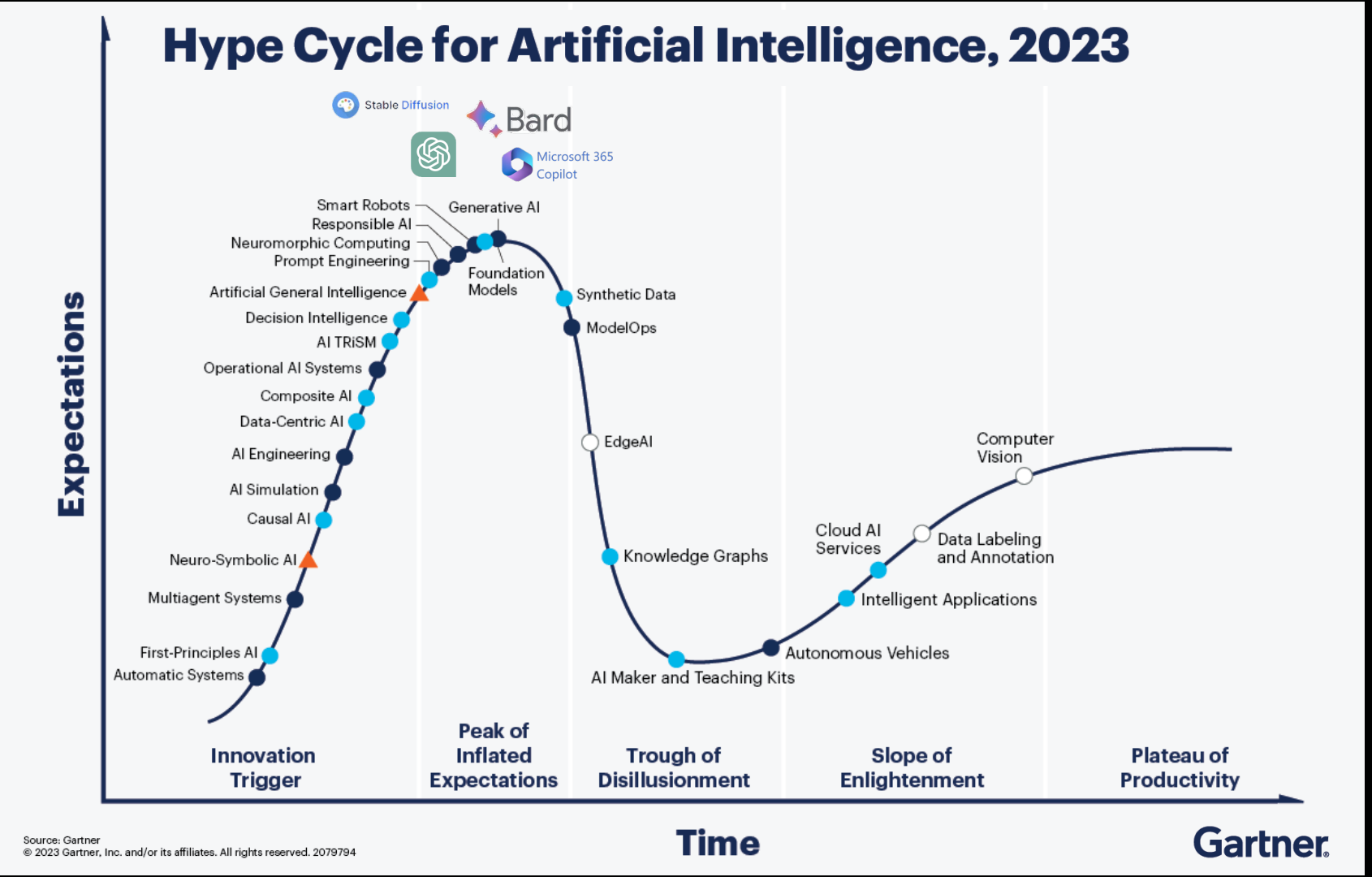
implications for the development of AI solutions in critical infrastructures

AI & Network Automation

AI and autonomous networks empowering the next digital transformation

AI & Network Automation

A new era – and we are only at the very beginning



AI & Network Automation

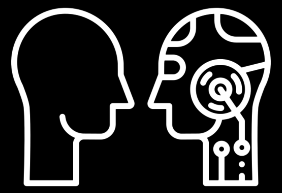
Opportunities: generative AI at the human-machine interface

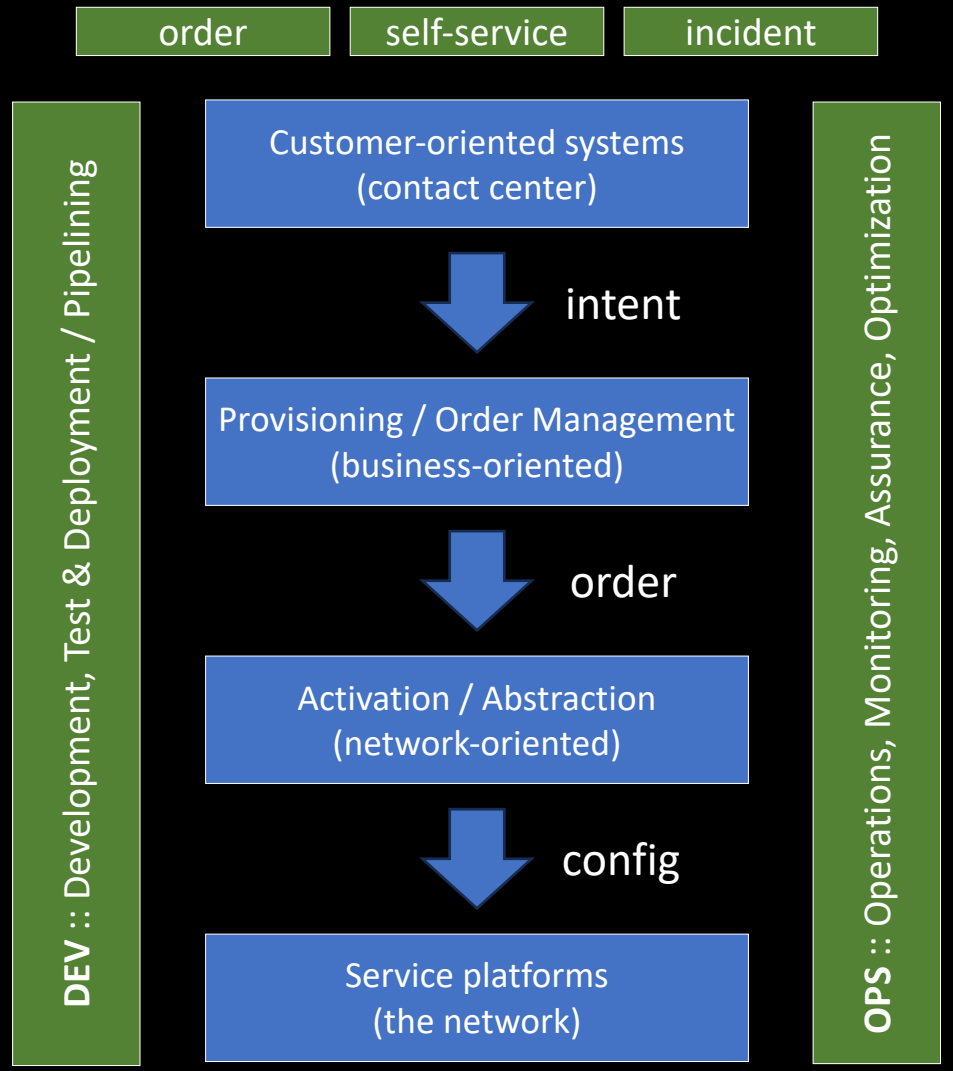
Assistance in the development of IT systems [OFFLINE usage]

Support of coding work / algorithmics during implementation

- Lifecycle / governance of interfaces and data models
- Creation of test cases
- Generation of documentation
- Basically: Takeover of recurring and easily formulated work

➔ Needs an adjustment period
➔ Potential for higher productivity
➔ Allows human concentration on the “tricky cases”





Customer interface with natural language [ONLINE usage]

- Order and advice
- Incident management with voice-controlled analysis and fault recording
- Self-service interface for individualizing the service

Operations & monitoring [ONLINE usage]

- Formulating queries for status and performance data
- Generation of KPIs and metrics

Additional ML techniques for prediction, anomaly detection, planning, security, etc. while operating the network

AI & Network Automation

Risks of proprietary solutions – especially when working with sensitive data

Companies

restrict usage by policies for protection

- Don’t input any personally identifiable information
- Don’t input any sensitive information
- Don’t input any company IP
- Do turn off history
- Do closely monitor outputs, which might suffer subtle but meaningful hallucinations, factual errors and biased or inappropriate statements.

Supplier

- Tailoring and enhancement of own solutions is limited by the closed and proprietary solution of the dominating players
- Development and integration of AI enabled services and products usually contradict compliance and NDAs
- Experimentation and qualification is difficult in a closed environment

Possible Option

- Open-source models could provide the needed flexibility and transparency
- Private Hosting provides the required privacy

GESCHÄFTSGEHEIMNISSE

Apple verbietet Nutzung von ChatGPT und Github Copilot

Apple lässt sich traditionell nicht in die Karten gucken. Das hat Konsequenzen für Mitarbeiter, die ChatGPT und Copilot von Github nicht nutzen dürfen.

in Pocket speichern | merken | 19. Mai 2023, 13:45 Uhr, Michael Linden

CHATGPT

Samsung verbietet Mitarbeitern die Nutzung generativer KI

Samsung Electronics hat ernst gemacht und seinen Mitarbeitern verboten, generative KI wie ChatGPT zu nutzen, weil Firmendaten geleakt wurden.

in Pocket speichern | merken | 2. Mai 2023, 11:15 Uhr, Michael Linden

Verizon announced that ChatGPT 'is not accessible from our corporate systems' in an effort to limit the 'risk of losing control of customer information' and source code

Don’t share sensitive info

Chat history may be reviewed or used to improve our services. Learn more about your choices in our Help Center.

the European AI Act (AIA)

implications for the development of AI solutions in critical infrastructures

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

EU AI Act [AIA]

Timeline

February, 2020
White Paper on Artificial Intelligence - A European approach to excellence and trust

April, 2021
First proposal of the EU AI Act by the European Commission

December, 2022
Council of the EU approved a compromise version

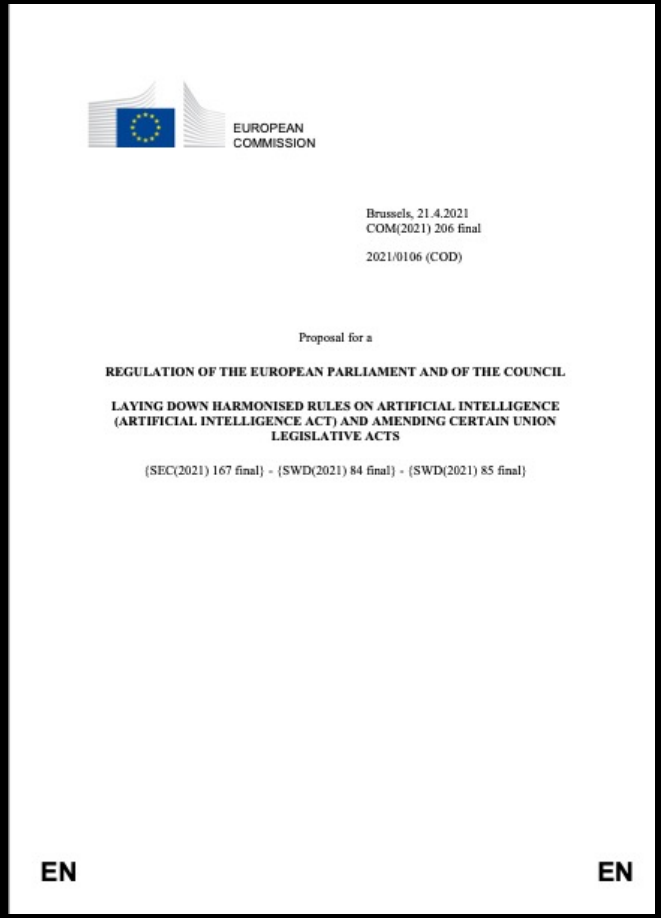
May, 2023
The EU parliament Committees approve the EU AI Act draft

June 14, 2023
Vote in the EU Parliament: MEPs adopted the negotiating position on the AI Act. Followed by talks within all EU countries in the Council on the final form of the law. (“Trilogue”)

:: WE ARE HERE ::

by the end of 2023
Approval upon agreeing the final text, start of the 2-year grace period

by the end of 2025
AI Act comes into effect


EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

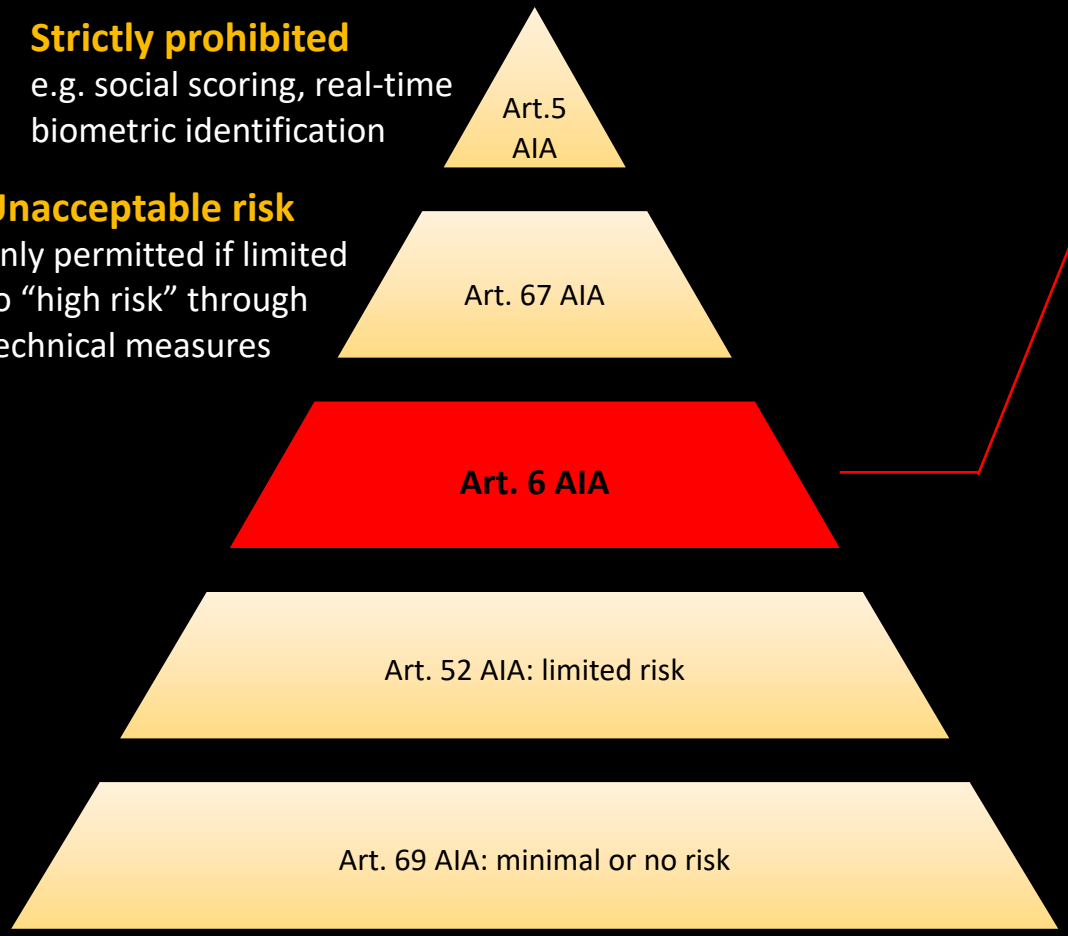
EN EN

EU AI Act [AIA]

Core rule: different rules for different risk levels

Strictly prohibited
e.g. social scoring, real-time biometric identification

Unacceptable risk
only permitted if limited to “high risk” through technical measures



AI systems identified as high-risk (Art. 6 AIA)

- Management and operation of critical infrastructure, specifically named in the AIA: road traffic and the supply of water, gas, heating and electricity
- To be expected / at the latest with the following national legislation for German, keyword KRITIS: ITC infrastructure, cloud services, data centers, communication networks

- Biometric identification and categorization of natural persons
- Education and vocational training
- Employment, worker management and access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Assistance in legal interpretation and application of the law

EU AI Act [AIA]

Some (!) requirements on AI systems identified as high-risk

Documentation

There must be automated logging of operations and comprehensive technical documentation

➔ common and already necessary for many systems today

Risk management

Risk management must be set up for the purpose of identifying, assessing and reducing risks

➔ should be feasible: might be challenging in individual cases, but common and already necessary for many systems today

Model / information design

Designing the model to prevent it from generating illegal content

➔ difficult, in any case extremely resource-intensive, and certainly never fully guaranteed

Data transparency

Obligation to provide summaries of copyrighted data used for training

➔ In principle it is feasible, but in any case, it is again a complex hurdle in terms of concrete implementation

Data quality

Data used for training, testing, and validation must be relevant, representative, free of errors and complete

➔ a purely theoretically achievable goal with the currently popular models

EU AI Act [AIA]

Timeline

February, 2020
White Paper on Artificial Intelligence - A European approach to excellence and trust

April, 2021
First proposal of the EU AI Act by the European Commission

December, 2022
Council of the EU approved a compromise version

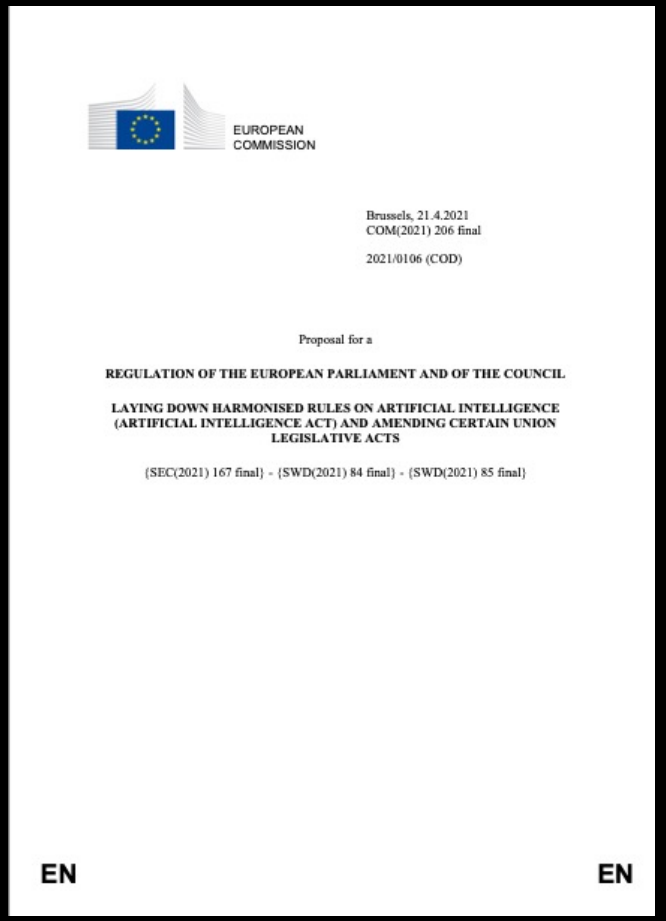
May, 2023
The EU parliament Committees approve the EU AI Act draft

June 14, 2023
Vote in the EU Parliament: MEPs adopted the negotiating position on the AI Act. Followed by talks within all EU countries in the Council on the final form of the law. (“Trilogue”)

:: WE ARE HERE ::

by the end of 2023
Approval upon agreeing the final text, start of the 2-year grace period

by the end of 2025
AI Act comes into effect


EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EN EN

EU AI Act [AIA]

Oh my god - what happened there?

30, 2023

Open letter to the repre
Commission,
Parliament

Artificial Intelligence
avant-garde

As engaged stakeholders o
serious concerns about the
the draft legislation would
sovereignty without effectively

e·on Capgemini SIEMENS orange Continental Henkel RENAULT Heraeus DANONE ONE PLANET. ONE HEALTH Schneider Electric united internet bitkom Carrefour Heineken UBISOFT

EU AI Act [AIA]

Timeline

by the end of 2025
AI Act comes into effect

3 years !

… and if ChatGPT hadn't made a breakthrough in the general public perception of AI, perhaps nothing would have happened to this day ...

June 14, 2023
Vote in the EU Parliament: MEPs adopted the negotiating position on the AI Act. Followed by talks within all EU countries in the Council on the final form of the law. (“Trilogue”)

The main risks related to the use of AI concern the application of rules designed to protect fundamental rights (including personal data and privacy protection and non-discrimination), as well as safety[32] and liability-related issues.

[32] This includes issues of cybersecurity, issues associated with AI applications in critical infrastructures, or malicious use of AI.

February, 2020
White Paper on Artificial Intelligence - A European approach to excellence and trust

EU AI Act [AIA]

Preliminary conclusion

1. **It is still unclear what exactly the AIA will look like at the end of the trilogue.** There will probably still be adjustments and deviations / differences in how national legislation will implement the act.

2. **Europe will not (may not?) allow an "unregulated use" of AI in critical areas.** Critical infrastructures will be protected and fenced off. No unreflective use of models whose origins, contents or effects are not transparent. Also because the EU has made mistakes in such areas in the past, think of Huawei and the 5G mobile core.

3. **On the other hand, Europe will try not to fall behind the US and Asia even further than it already does.** We will see, if initiatives like LEAM.AI will become a success (in my opinion: not really, far too little money, far to slow).

4. **Operators of critical infrastructures must consider what type of AI solution they allow in their networks** – against the AIA background shown: interesting short-term approaches can quickly turn into unmanageable complexity. The closer to the network, the higher the requirements for transparency and sovereignty over the AI solution will be.

5. **The best for now: building up competence.** Be a maker instead of just a user. Experiment with your own, local, controllable AI solutions, based on open pipelines and open models, with a focus on transparency.

Become a maker: Get involved. Come around.

Experience the XyPilot live and in color.

XyPilot is an AI assistance system for programming / algorithms in process automation.

- Based upon open components
  ➔ documentation + model design
- Operated in a local environment (private cloud)
  ➔ control, privacy, security
- Retrained for specific context - without information leaking into uncontrollable environments
  ➔ data transparency
- Seamless integrated into a process automation platform
  ➔ really useful
- Outlook: we work on enhancements, e.g. a security layer and automated qualitative metrics
  ➔ greater reliability for use in critical infrastructures

13:30 – 15:15 **Room C19/3**

Pair-Programming with AI?! (Presentation)

Sebastian Brummer

Moritz Schrauth

Xyna GmbH

Room C19/3

Pair-Programming with AI?! (Mini-Workshop)

Sebastian Brummer

Moritz Schrauth

Xyna GmbH

Room C19/3

Thank you.