

From: [REDACTED]
To: [REDACTED]
Subject: Re: ACK: Request for a meeting - CCIA position paper on AI Act
Date: mardi 11 janvier 2022 15:34:33

Dear [REDACTED],

26/01, 16:00-16:30 would work for us. If possible we would prefer by zoom

Many thanks!

I will wait for your invitation,

Best regards,

[REDACTED]

On Tue, Jan 11, 2022 at 1:04 PM [REDACTED]
[REDACTED] <[\[REDACTED\]@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)> wrote:

Dear [REDACTED]

Thank you for your swift reply. I have the pleasure to transmit Mr Stengg's availability for a virtual meeting (and with email I answer as well to the meeting request with the same topic sent to his attention) on the following possible dates:

25/01, 11:00-11:30/ 16:30-17:00

26/01, 16:00-16:30

Please communicate your preference for a suitable date and also for a video platform you would like to use.

For transparency purposes, this meeting will be published in the Transparency Register of the European Commission. Please make sure your organisation is duly registered.

The Cabinet does not intend to communicate actively on the content of this meeting. However, in line with Regulation (EC) No 1049/2001, minutes can be made accessible to the public upon request (without any disclosure of protected interests).

Looking forward to hearing from you.

With kind regards,

[REDACTED]

[REDACTED]

[REDACTED]



European Commission

[REDACTED]

B-1049 Brussels/Belgium

[REDACTED]

[REDACTED] [@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)

From: [REDACTED] [@ccianet.org](mailto:[REDACTED]@ccianet.org)

Sent: Monday, January 10, 2022 3:35 PM

To: [REDACTED] (CAB-VESTAGER) <[\[REDACTED\]@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)>; [REDACTED]
<[\[REDACTED\]@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu)>

Subject: Re: ACK: Request for a meeting - CCIA position paper on AI Act

Dear [REDACTED],

Many thanks for your reply. We fully understand the tight agenda, however, we would be very much delighted to meet Mr Werner Stengg instead.

Dear [REDACTED],

Please feel free to send me some time slots that could work for Mr Werner.

Many thanks in advance

Kind regards,

[REDACTED]

On Mon, Jan 10, 2022 at 2:46 PM [REDACTED] [@ec.europa.eu](mailto:[REDACTED]@ec.europa.eu) wrote:

Good afternoon,

On behalf of Kim Jørgensen and Christiane Canenbley, thank you for your meeting request. As their agenda is full in the weeks to come, we suggest a meeting with Digital Expert Werner Stengg instead. Kindly liaise with my colleague [REDACTED] in copy to find a suitable date for the meeting. Thanks.

Kind regards,

[REDACTED]

European Commission

Cabinet of Executive Vice-President Margrethe VESTAGER

[REDACTED]

[REDACTED]

Rue de la Loi, 200

B-1049 Brussels

phone: [REDACTED]



European Commission

Fra: [REDACTED] <[REDACTED]@ccianet.org>
Dato: 5. januar 2022 kl. 12.21.17 CET
Til: "JORGENSEN Kim (CAB-VESTAGER)"
<xxx.xxxxxxxxxx@xx.xxxxxx.xx>
Cc: [REDACTED] <[REDACTED]@ccianet.org>
Emne: Request for a meeting - CCIA position paper on AI Act

Dear Mr Jorgensen,

I hope this email finds you well.

I am writing to you on behalf of the Computer & Communications Industry Association (CCIA Europe) to kindly request a virtual meeting to discuss the Commission's proposal on the Artificial Intelligence Act.

Please also allow me to share CCIA Europe's new position paper on the AI Act. CCIA has long supported and welcomed the Commission's proposal. We do however, find that a few aspects of the proposal deserve further discussion e.g. the broad scope of some definitions, unclear bans on AI systems (facial recognition), prescriptive mandatory requirements, and unequal distribution of responsibilities across the AI value chain. We would also like to share with you (below in red) some suggestions for amendments to Articles 3, 5, 6 and Annex III as well as some concerns regarding the compromise text prepared by the Slovenian presidency.

We are flexible in terms of the timing, so please feel free to suggest a date and time that works for you. We suggest opening up this virtual meeting to a few CCIA members.

I look forward to hearing from you, and please be in touch if you have any questions.

Kind regards,

[REDACTED]

Article 3.1

For the purpose of this Regulation, the following definitions apply:

1. 'artificial intelligence system' (AI system) means software *that uses models* that is developed with one or more of the techniques and approaches listed in Annex 1 *and can, for a given set of human-defined objectives, generate outputs such as content, to make predictions, recommendations, or decisions, or to generate content, influencing the environments they interact with without any independent human judgement;*

ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

(a) Data driven Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Classical AI techniques *Logic and knowledge-based approaches*, including knowledge representation, inductive (logic) programming, knowledge bases, *inference and deductive engines* (symbolic) reasoning and expert systems;

(c) Classical and modern statistical approaches *to learning and inference, including linear and logistic regression, Expectation Maximization estimation, Bayesian estimation and inference, probabilistic graphical models, and high-dimensional data analysis methods such as principal components analysis search and optimization methods.*

Article 5.1

1. The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or Implementing for use of an AI system that intentionally deploys subliminal techniques beyond a person's consciousness in order with the objective to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person material physical or psychological harm;

(b) the placing on the market, putting into service or use of Implementing for use an AI system that intentionally or could reasonably foreseeably exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person material physical or psychological harm;

Article 6

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both the following conditions are fulfilled:

the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II **and the AI system must make final decisions that create a material adverse risk to a person's fundamental rights or health and safety.**

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk **if they make final decisions that create a material adverse risk to a person's fundamental rights or health and safety.**

ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6

1. Biometric identification **systems and categorisation of natural persons:**

(a) **Biometric identification systems** intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons **without their express or implied agreement;**

2. **Management and operation of** critical infrastructure:

(a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

With regards to the revisions in Annex III presented in the **compromise text prepared by the Slovenian Presidency of the Council**, we note with concern the introduction in Annex 3 (2) (aa) of 'AI systems intended to be used to control or as safety components of digital infrastructure.' This inclusion is overly broad, as it is undefined and could include things like computer code, software, hardware, the cloud, and the internet. Digital infrastructure can support critical functions (like operation of traffic, water, gas, etc. mentioned in subsection a, but it also supports many things which are low risk (such as video and music streaming services, computer games, online videos, and web browsing). Importantly, AI plays a fundamental role in how

digitally native offerings are run. By categorizing every AI system that controls or secures digital infrastructure as high risk, policymakers would vastly overregulate this space and stifle innovation in the cloud. Companies would be required to comply with the high risk requirements to make small improvements to digital infrastructure, even where the impacts are low risk.

For example, a small business might develop personal computer games. If the business uses an AI system to help write, improve, and ensure security of that code, it would seem like an unintended consequence to subject the AI system to high risk requirements. Or, if a store changes its website, it may use an AI system to help redirect web traffic to the proper corresponding updated pages. Again, it would seem like an unintended consequence to subject that AI system to high risk requirements.

Second, existing legislation and the existing high-risk categories should capture policymaker's concerns about digital infrastructure high risk use cases. There are already laws specifically focused on ensuring the security of digital infrastructure where appropriate. Moreover, laws around personal data and data security, like GDPR, apply to how digital infrastructure processes personal data. And as already noted, critical infrastructure like operation of road traffic and the supply of water, gas, heating and electricity is already covered in preceding high risk categories.

Finally, **to the extent AI systems are used to assist in controlling or securing digital infrastructure, such cutting-edge techniques should be encouraged and promoted in order to ensure the EU does not fall behind the rest of the world in privacy and data security.** Placing burdensome requirements on use of that technology without real, demonstrated risk that those systems cause harm could put the EU at a disadvantage and prevent it from accessing the most innovative and secure methods for controlling and securing technology.

--

[REDACTED]

[REDACTED]

Computer and Communications Industry Association (CCIA Europe)

[Rue de la Loi 227, 1st floor, 1040 Brussels, Belgium](#)

EU Transparency Register number: 15987896534-82

email: [REDACTED]@ccianet.org

mob: [REDACTED]

