European Center for
Not-for-Profit Law

EPICENTER
.WORKS
for digital rights

To: Staatssekretär Florian Tursky
Bundesministerium für Finanzen
Johannesgasse 5
1010 Wien

8. August 2023

Dear State Secretary Tursky,

Our two organisations want to highlight important shortcomings in the current trajectory of the AI Act and call on Austria to stand up for a future proof EU law that protects human rights.

National Security exemption in the proposed EU AI Act

We welcome the Austrian government's human and ethics focused approach to the regulation of AI. We especially support and further encourage the inclusion of civil society, the focus on risk prevention, sovereignty, „ethics by design", „privacy by design" and „security by design" and a use of AI that benefits all of society. However, to ensure this, we would like to express our serious concern with the current EU Council position which would weaken human rights safeguards in the proposed EU Artificial Intelligence Act (AIA). Given the potential human rights implications both within the EU and globally, we call on the Austrian Government to continue the dialogue with legal and human rights experts to review the Council's position on national security ahead of the start of trilogue negotiations.

Moreover, we would like to draw attention to three key aspects of the Austrian government's current AI strategy – health, education and mobility.

At the EU Telecommunications Council on 6 December 2022, all EU Member States including Austria agreed to adopt a General Approach on the AIA, which will form the basis for trilogue negotiations later this year with the European Parliament. This General Approach notably amends the original European Commission proposal and introduces a new blanket exemption for AI systems placed on the market, put into service, or used for the purpose of "national security".

Such a blanket exemption introduces a significant loophole that would automatically exempt certain AI systems from scrutiny and limit the applicability of human rights safe guards. Many NGOs have strongly opposed this exemption in Brussels[1]. Moreover, the UN Special Rapporteur on Human Rights and Counter-Terrorism has explicitly called for the removal of the national security exclusions in the AIA, warning of "*a terrible precedent regionally and globally*"[2]. Polling carried out across 12 EU member states has also shown that the use of AI for national security is an issue of serious public concern[3] and investors have raised their own concerns, supporting the regulation of AI for national security[4].

1 '*Ensure fundamental rights protections in the Council position on the AI Act*' EDRi letter to Czech Presidency of the EU, 17 October 2022 https://edri.org/wp-content/uploads/2022/10/CZ-Minister-Digitalisation-letter-AI-act.pdf

2 '*Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*' Report to the 52nd session of the UN Human Rights Council, 1 March 2023 https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session52/advance-version/A_HRC_52_39_AdvanceEditedVersion.docx

3 '*New Poll: Public fears over government use of Artificial Intelligence*' ECNL, 14 November 2022 https://ecnl.org/news/new-poll-public-fears-over-government-use-artificial-intelligence

4 '*Investor statement in support of digital rights regulations*' Investor Alliance for Human Rights, 15 February 2023 https://investorsforhumanrights.org/sites/default/files/attachments/2023-02/FINAL%20Investor%20Statement%20AI%20Act%20w-signatories%202-14-23_0.pdf

As civil society has warned, a blanket exemption based on vague national security grounds will also prevent

> *"effective public transparency about the use of high-risk systems in the areas which have perhaps the most severe impact on fundamental rights*[5]*."*

Lack of transparency consequently denies people impacted by AI systems the right to challenge potentially life-changing decisions and seek remedy and redress in case of harm and could violate their right to a fair trial[6].

We are not aware of any opposition raised in Council to the need for human rights safeguards in the development of AI for national security in principle, or any questioning of the relevance of international human rights law in this area. We understand that the proposed exemption has been agreed on by Council due to concerns raised over EU competence on national security issues, although this is legally disputed[7] and requires detailed examination. EU case law has established that

> *"although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law"*[8]*.*

We therefore call on the Austrian government to initiate a discussion to reconsider the blanket national security exemption in the Council General Approach.

The other aspects concern the Austrian national AI strategy:

Firstly, the field of education is concerned. Especially children should have a safe space where they can learn and develop their personality. "*Predictive analytics*" to help pupils learn,[9] however, can lead to unwanted profiling with all its biases and potentially huge negative consequences. The issue lies in the (in-)ability to give consent, in extensive collection and processing of highly sensitive personal data, potential discrimination of individuals within and outside the learning environment by private or state actors and security risks regarding hacking. Even if a child or parent consents, all the other risks remain and later (career) wishes of the child could be influenced by these profiles – generated from data collected during the most sensitive phase of personal development. **We therefore ask to ban predictive analytics in schools.**

Secondly, the area of health must be treated very carefully. Even though AI might help practitioners or improve diagnostics,[10] people shall **not be obliged to use** health apps or wearables or provide health data in other ways in order to have it analysed by AI. Everybody must have the simple choice to **opt**

5 '*Ensure fundamental rights protections in the Council position on the AI Act*' EDRi letter to Czech Presidency of the EU, 17 October 2022 https://edri.org/wp-content/uploads/2022/10/CZ-Minister-Digitalisation-letter-AI-act.pdf

6 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, Official Journal L 142, 1.6.2012, p. 1–10, http://data.europa.eu/eli/dir/2012/13/oj

7 '*Legal Opinion on the implications of the exclusion from new binding European instruments on the use of AI in military, national security and transnational law enforcement contexts*' Prof. Douwe Korff, 18 October 2022 https://ecnl.org/news/rights-free-zone-blanket-national-security-exemption-ai-legislation

8 Judgment of the Court (Grand Chamber) in Case C-623/17, 6 October 2020 https://curia.europa.eu/juris/document/document.jsf;jsessionid=DC1C6EE6335FCFE02B5D540D7C610EA2?text=&docid=232083&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2401090.

9 https://www.bmk.gv.at/dam/jcr:98f59eaf-006f-4885-b2ed-6d2c8b6806c7/AIM_AT_2030_Annex_UA.pdf , p. 22 et seqq.

10 https://www.bmk.gv.at/dam/jcr:98f59eaf-006f-4885-b2ed-6d2c8b6806c7/AIM_AT_2030_Annex_UA.pdf , p. 17 et seqq.

out of such a system **without being discriminated against** in the health system. Austria has championed this approach with the ELGA opt-out and people expect the same good standard to be uphold. Wherever possible, patient data must be processed **anonymised or pseudonymised, which is often not even the case in third party use (scientific access, EU Health Data Space, etc.)**. Importantly, every patient must be **protected from third parties that are not directly involved in their treatment accessing the data and from potential security threats** in case this highly sensitive data is leaked etc.

Thirdly, precautions regarding AI & mobility need to be taken. This includes real-time analysis and on-demand solutions for example of information on when and where passengers use which means of transport. Merging vehicle-specific data with mobile phone data of passengers can lead to profiling as well as automated decisions about how many people get on at different stops and which recommendations for which vehicle is best suited to meet the individual's travel needs, and with this to GDPR issues.[11] The GDPR prohibits automated decisions based on profiling without consent. This is why, we ask to prohibit the analysis of individual's travel behaviour.

We would be very happy to meet with you to discuss this important matter, or to provide further information or clarification.

Yours sincerely,

Epicenter.works – for digital rights
Thomas Lohninger
Executive Director
Vienna, Austria

European Center for Not-for-Profit Law Stichting (ECNL)
Vanja Skoric
Program Director
The Hague, Netherlands

11 https://www.bmk.gv.at/dam/jcr:98f59eaf-006f-4885-b2ed-6d2c8b6806c7/AIM_AT_2030_Annex_UA.pdf, p. 8.