AK EUROPA

AMENDMENTS

Need for improvement to the draft Artificial Intelligence Act from the consumer's point of view

ANNEX: Recommended Amendments to Art 53 – 54a of the AIA Proposal

AI regulatory sandboxes and testing of high-risk AI in real world conditions

Overall, the regulations on both real laboratories and real-world testing pose far too many risks for those concerned to remain uninformed, not to be involved voluntarily, suffer disadvantages and damage, not to find any points of contact for questions and complaints, and not to be professionally supported and supervised throughout the process. Against this background, we are primarily in favour of deleting the chapter without replacement, or at least for a fundamental revision of the chapter from the perspective of protecting the interests of those affected.

Art 53 – AI regulatory sandboxes

Amendment to para 1: The passage „...and, where appropriate, in cooperation with other relevant national authorities, or by the European Data Protection Supervisor in relation to AI systems provided by the EU institutions, bodies and agencies" should be replaced by: „The EU Data Protection Supervisor (EDPS) must be consulted whenever personal data are to be processed in a real laboratory in accordance with the GDPR. Cooperation with the national data protection authority, which can impose conditions and issue prohibitions, must be ensured in this regard."

Reason: The involvement of the EU Data Protection Supervisor (EDPS) is welcomed. However, there should be legal certainty as to the cases in which he/she is to be included. „Where appropriate" in any case does not have the desired degree of certainty. From our point of view: whenever personal data are processed in the real lab and in cooperation with the national Data Protection Authorities (DPA).

Addition in para 1a: The passage „The national competent authority or the European Data Protection Supervisor, as appropriate, may also supervise testing in real world conditions upon the request of participants in the sandbox" should be replaced by: „Those responsible for ‚real-world testing' are responsible for consulting the supervisory authorities responsible for AI and data protection even before the project begins. The supervisory bodies may impose conditions and issue prohibitions in order to guarantee that the activities are carried out in compliance with the law. In addition, the EU Data Protection Supervisor (EDPS) must be consulted if personal data are to be processed in a real laboratory in accordance with the GDPR."

Reason: Upon request, national supervisory authorities or the EDPS may also be involved in the work of „real-world testing" under Art 54a if participants wish so. In the absence of a definition, it is first necessary to specify, who the participants are that can make this request. Presumably, this means companies and research institutions. It is not clear from the phrase „may also supervise" whether the supervisory bodies addressed must comply with the request. In view of the damage potential of high-risk applications, we are in favour of mandatory involvement of the competent supervisory authorities and the EDPS even in the absence of a request.

Deletion without replacement in para 1b: the passage: „a) foster innovation and competitiveness and facilitate the development of an AI ecosystem" should be deleted.

Reason: As long as the regulations seem to exempt real labs from compliance with the legal framework (AI, product safety and liability, parts of the GDPR) to a certain (and otherwise ambiguous) extent, the

reasons for establishing real labs must be exclusively in the public interest. A) Against this backdrop, "foster innovation and competitiveness…" should be deleted without replacement.

Addition in para 2: To the passage „As appropriate, national competent authorities may allow for the involvement in the AI regulatory sandbox of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs and innovation hubs" should be added:
„Representatives of those affected, such as consumer associations, patients' advocates, NGOs committed to civil rights, are to be nominated by the competent supervisory authorities and, in any case, are to be involved in the project in an advisory capacity."

Reason: Incomprehensibly, regulators are allowed to consult other stakeholders „where appropriate" (including standards institutes, notified bodies, and researchers) but not representatives of stakeholders, such as – but by no means limited to – consumer organisations, patient advocates, civil rights NGOs, and others.

Addition in para 2a: The passage „Participation in the AI regulatory sandbox shall be based on a specific plan agreed between the participant(s) and the national competent authoritie(s) or the European Data Protection Supervisor, as applicable. The plan shall contain as a minimum the following:" should be supplemented with section (f) „The submission plan shall describe which natural/legal persons will be involved in the experiment, how data subjects within the meaning of the GDPR will be informed, how their data protection consents will be obtained and demonstrated, and where data subjects can turn to with their enquiries and complaints."

Reason: The paragraph describes the submission plan for real labs. Again, any reference to the people affected by the experiment is lacking. In order to comply with the right to digital self-determination, participants must explain whom they intend to include in the trial, how they have informed the data subjects of their plans, how their data protection consents have been obtained and proven, and where people can turn with enquiries and complaints.

Amendment to para 4: The passage „The participants remain liable under applicable Union and Member States liability legislation for any damage caused in the course of their participation in an AI regulatory sandbox" should be replaced by: „ Regardless of fault, participants are liable for any material or immaterial damage to property, persons, or assets incurred in the course of the test."

Reason: The reference to participants remaining responsible for any damage caused, recognised under national/EU law, falls short. We refer to the revision work on the Product Liability Directive and the need for strict liability, which is being discussed in this context. In the given context (affected persons who are „forced against their will"), pure fault-based liability is unacceptable.

Article 54 – Further processing of personal data in AI „sandboxes/real labs"

Deletion in para 1 of the passage „increase in efficiency in the administration" and addition of the passage: „Data subject rights under the GDPR can also not be excluded by referring to processing interests under Art 89 GDPR. The companies or institutions responsible for a real laboratory, in particular, must inform the persons affected by data processing under the GDPR of such a project in accordance with Art 12 et seq. GDPR and obtain GDPR-compliant consent. The competent data protection authority must examine such a project in advance; in particular the existence of effective consents from the test participants and impose appropriate conditions or prohibit the project if it cannot be carried out in compliance with the GDPR."

Reason for deletion: Amongst the requirements is proof of a public interest related to a health, public safety, environmental application „or an increase in administrative efficiency". The latter is such a broad catch-all term that any conceivable public task could be subsumed under it. In view of our concerns regarding fundamental rights expressed at the beginning, the scope of application should be made more precise or deleted without replacement.

Reason for addition: In so-called AI real labs, personal data that was actually collected for other purposes may be used for testing AI if there is a significant public interest (in the prosecution of criminal offences, with regard to health or the environment) and anonymous data is not sufficient to cover it. From AK's point of view, this provision undermines the GDPR in an unacceptable way: Article 6(4) of the GDPR sets tight limits on further processing of data for another purpose. Against this background, those affected would have to be informed of such a project and their consent obtained. Disregarding the right to self-determination of the persons concerned over their personal data, appears to be contrary to fundamental rights and would probably not stand up to scrutiny by the European Court of Justice. It is true that „it is necessary to monitor whether there are high fundamental rights risks during testing".

From the AK's point of view, people cannot be exposed to this risk for testing purposes without being asked. Explicit consent needs to be made available to test subjects. The data protection authority must examine such a project in advance and impose appropriate conditions or prohibit the project if it cannot be carried out in compliance with the GDPR.

The fact that monitoring is to be carried out to determine whether „high risks to fundamental rights" arise in the real laboratory is not enough. The fact that a project stop may be necessary also does not create appropriate legal safeguards. Involvement of the DPA/ EDPS is, after all, only at the request of the project managers. Whether/how exactly affected parties learn that they are involved in a project is not clear from the draft. Fundamental rights guarantees must therefore be significantly strengthened. Lit f) states that data subjects' rights under the GDPR are not affected, i.e. that there is at least a right to information, disclosure, rectification and deletion. With regard to the opening clause in favour of science and research in Art 89 GDPR, it should be specifically noted that data subject rights cannot be excluded under the GDPR. From our point of view, a departure from the requirement of data subjects' consent to data processing is disproportionate. Art 53 et seq. cannot create a new legal basis for an interference with data protection if only because particularly protected health data can be processed and the protection guarantees required by the GDPR are lacking.

Deletion of para 1a without replacement: The passage „For the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of law enforcement authorities, the processing of personal data in AI regulatory sandboxes shall be based on a specific Member State or Union law and subject to the same cumulative conditions as referred to in paragraph 1" should be deleted without replacement.

Reason: Even assuming a separate subject matter law, real-world laboratories that use real human AI data to prevent and prosecute crimes are hardly justifiable from a fundamental rights and ethical perspective.

Art 54a – Testing of high-risk AI systems in real world conditions

Deletion in para 1: The passage „The detailed elements of the real-world testing plan shall be specified in implementing acts adopted by the Commission in accordance with the examination procedure referred to in Article 74(2)" should be deleted in favour of detailed regulations in the AIA.

Reason: The regulation of important details of „real-world testing" in delegated acts should be rejected.

Para 3: In the passage „The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to ethical review that may be required by national or Union law" it should be noted that this competence is most likely to be assigned to (constitutional) courts.

Reason: The fact that the test is carried out subject to a statutory „ethical review" leaves many questions unanswered. Who, when, how decides whether such a testing project is even remotely compatible with basic ethical principles?

Amendments to para 4: In „(b) the market surveillance authority in the Member State(s) where the testing in real world conditions is to be conducted or to the European Data Protection Supervisor, as applicable, have not objected to the testing within 30 days after its submission" the period of 30 days should be extended to 90 Days. Section (g) should be replaced by „Only persons with their effective consent who meet certain minimum requirements set by the supervisory authority may participate in the test".

Reason: The appeal period for the EDPS of 30 days is way too short. Furthermore, the question arises whether and in which cases the national DPAs also have a right of appeal (or why not at all). That no „vulnerable" individuals can participate in the test is too imprecise. Who decides who belongs to vulnerable groups? It has been sufficiently scientifically processed that every citizen/consumer is vulnerable in some way. Simply because the information that forms the basis for consent to participate under Art 54b overwhelms the average citizen, affected individuals are vulnerable because they do not engage in the experiment knowing the implications.

ANNEX: Consolidated Recommended Amendments to the AIA Proposal

Recitals

It is recommended to clarify in the Recitals that the notion of 'fundamental rights risks' may include economic risks and risks for society at large. 'Fundamental rights' are often understood as specifically meaning individual rights listed in the Charter (see 7.2.2 and 7.2.3), which might give rise to the misunderstanding that risks such as fraud or the undermining of democratic elections are not covered. From a consumer perspective, the inclusion of economic risks and societal risks is definitely of key importance.

[…] Whereas: […]

(32) As regards stand-alone AI systems, meaning high-risk AI systems other than those that are safety components of products, or which are themselves products, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in the Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems. **The notion of fundamental rights risks is understood very broadly and not restricted to risks for rights explicitly mentioned under a separate Article in the Charter as long as there is a sufficient link between the risk and enjoyment of rights under the Charter. Notably, the notion of fundamental rights risk may, depending on the context, include mere economic risks where those risks are sufficiently severe, for instance because they affect access to essential goods or services (such as energy supply, credit or insurance) or because they operate on a large scale and may significantly affect the general standard of living of a natural person (such as large scale personalised pricing). The notion of fundamental rights risks also includes risks for society at large, such as for democratic institutions and a fair and open discourse.**

[…]

Definitions

It is important to detach the definitions of 'emotion recognition system' and 'biometric categorisation system' from the definition of 'biometric data', which has been copied from the GDPR and requires that the data allow or confirm the unique identification of a natural person. Emotion recognition and biometric categorisation, however, do not (necessarily) rely on personal data that allow or confirm the unique identification of a particular individual. It is therefore recommended to introduce a separate definition of 'biometrics-based data' (see 6.3.1).

It is also important to modify the notion of 'real-time' in the context of remote biometric identification because the pivotal point is not so much the duration of delay between capturing of live templates and identification but rather whether identification occurs on a large scale over a period of time (see 6.2.1.3). Where this is not the case and identification is just limited to a particular past incident, such as a crime captured by a video camera, we may not need the same strict regulation as for real-time remote identification.

Further suggestions as to concrete formulations have been made as stated above, but these are of lower priority.

Article 3

Definitions

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

[…]

(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(33a) 'biometrics-based data' means personal data resulting from specific technical processing relating to physical, physiological or behavioural signals or characteristics of a natural person, such as facial expressions, movements, pulse frequency, voice, keystrokes or gait, which may or may not allow or confirm the unique identification of a natural person;

(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions, **thoughts** or intentions of natural persons on the basis of their ~~biometric~~ **biometrics-based** data;

(35) 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories such as sex, age, hair colour, eye colour, tattoos, ethnic origin, **health, mental ability, personality traits** or sexual or political orientation, on the basis of their ~~biometric~~ **biometrics-based** data;

(36) 'remote biometric identification system' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without the conscious cooperation of **the persons to be identified** ~~prior knowledge of the user of the AI system whether the person will be present and can be identified ;~~

(37) ''real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur **on a continuous or large-scale basis over a period of time and without limitation to a particular past incident (such as a crime recorded by a video camera)**; ~~without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~

[…]

List of prohibited AI practices in Title II

It is recommended to broaden the scope of the three existing per se-prohibitions – manipulation by subliminal techniques, exploitation of vulnerabilities and social scoring – in several ways (see 5.1.1.3, 5.1.2.4 and 5.1.3.3). In particular, it is recommended to replace 'physical or psychological harm' by 'material and unjustified harm', both with the aim of including economic harm and of avoiding overreaching effects (see above the modifications in points (a) and (b)).

It is likewise recommended to extend the prohibition of exploitation of vulnerabilities from group-specific vulnerabilities to individual vulnerabilities, e.g. very individual personality traits discovered with the help of data analytics (see above point (b)), and to remove the restriction to public authorities in the prohibition of social scoring with a view to extending it to social scoring conducted by private actors, e.g. by a provider of a gatekeeper platform service (see above the modification in point (c)).

In terms of AI practices missing in the list of prohibited practices, it is recommended to add total surveillance (see 5.2.1) and violation of mental privacy and integrity (see 5.2.2) (see above new points (ba) and (bb)).
In any case, it is recommended to clarify that Article 5 needs to be seen in the context of a host of prohibitions

following from other law, which apply irrespective of whether AI is involved or not (see above paragraph 1a), and to allow for flexibility by empowering the Commission to update the list of prohibited AI practices by way of delegated acts (see above paragraph 1b)).

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5

1. The following artificial intelligence practices shall be prohibited:
   (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person ~~physical or psychological~~ **material and unjustified** harm;
   (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of
      (i) a specific group of persons due to their age, physical or mental disability **or social or economic situation;** or
      (ii) **an individual whose vulnerabilities are characteristic of that individual's known or predicted personality or social or economic situation**
   ~~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 ~~physical or psychological~~ **material and unjustified** harm;
   (ba) **the putting into service or use of an AI system for the comprehensive surveillance of natural persons in their private or work life to an extent or in a manner that causes or is likely to cause those persons or another person material and unjustified harm;**
   (bb) **the placing on the market, putting into service or use of an AI system for the specific technical processing of brain data in order to read or manipulate a person's thoughts against that person's will or in a manner that causes or is likely to cause that person or another person material and unjustified harm.**
   (c) the placing on the market, putting into service or use of AI systems ~~by public authorities or on their behalf~~ for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:
      (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
      (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;
   (d) *[to be moved to new Article 5a]*

1a. **In addition to the prohibited AI practices referred to in paragraph (1), AI practices referred to in Annex Ia shall also be considered prohibited. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex Ia on the basis of a similar threat to fundamental rights and European values as posed by the practices listed in paragraph (1).**

1b. **Paragraphs (1) and (1a) are without prejudice to prohibitions that apply where an artificial intelligence practice violates other laws, including data protection law, non-discrimination law, consumer protection law, and competition law.**

[Paragraphs 2 to 4 to be moved to new Article 5a]

Biometric techniques as 'restricted AI practices'

With regard to real-time remote biometric identification an entirely new regulatory approach has been suggested (see 6.2.2). As the provisions on real-time remote biometric identification do not resemble the per se-prohibitions in Article 5, but rather stipulate conditions for the use of these techniques, they should be moved to a separate Title IIa on 'Restricted AI practices'. As to the structure, the close interplay with Article 9 GDPR would become much clearer if the new provision were structured in a similar way and if explicit reference to the several justifications in Article 9 GDPR were made (see above paragraph 1). There should be a clarification that the new provisions do not in any way derogate basic principles of other laws, notably of the GDPR, such as that data must only be stored as far as strictly necessary to achieve the relevant law enforcement purpose (see above paragraph 5).

Given that real-time remote identification achieved with the help of other than biometric techniques (e.g. with the help of mobile phone signals) may be almost as problematic it could be an option to remove the restriction to biometric identification and include also other techniques of mass identification.

TITLE IIA

RESTRICTED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5a

'Real-time' remote biometric [Opt.: or other] identification

1. AI systems may be used for 'real time' remote biometric identification [Opt.: or other 'real time' remote identification] in publicly accessible spaces only when such surveillance is limited to what is strictly necessary for:

(a) the use for a specific purpose to which the persons identified have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;

(b) the use for purposes and under conditions referred to in Article 9 (2)(b) and (j) of Regulation (EU) 2016/679;

(c) the use for migration, asylum or border control management;

(d) the use ~~of 'real-time' remote biometric identification systems in publicly accessible spaces~~ for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific potential victims of crime, including missing children;

(ii) the prevention of a specific, substantial and imminent threat **to public security, in particular** to the life or physical safety of natural persons, or of a terrorist attack;

(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

2. The use of 'real-time' remote [biometric] identification systems in publicly accessible spaces for the purpose~~s of law enforcement for any of the objectives~~ referred to in paragraph 1 point**s c) and d)** shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote [biometric] identification systems in publicly accessible spaces ~~for the purpose of law enforcement~~ for any of the objectives referred to in paragraph 1 points

c) and d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point**s (c) and** (d) and 2, each individual use for ~~the purpose of law enforcement~~ of a 'real-time' remote [biometric] identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

   The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point**s (c) and** (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote [biometric] identification systems in publicly accessible spaces ~~for the purpose of law enforcemen~~t within the limits and under the conditions listed in paragraphs 1, point**s (c) and** (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point**s (c) and (**d), including which of the criminal offences referred to in point **(d)** (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

5. Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law and non-discrimination law, remain unaffected. In any case, only such personal data may be collected through remote biometric identification as are strictly necessary to achieve the purpose stated in paragraph (1), and must be erased as soon as they are no longer necessary in relation to this purpose.

As emotion recognition systems and biometric categorisation systems pose a significant threat to fundamental rights, and as they are currently not covered by Article 9 GDPR (but only by Article 6 GDPR), it is recommended to establish for these techniques a regulatory regime similar to that of Article 9 GDPR (see 6.3.2.3). This regime could then also include biometric identification that does not qualify as real-time remote biometric identification. It has been demonstrated in some detail why an 'Article 9 regime' would not be overreaching, at least not if a de minimis-exception is added (see paragraph 2 above). If such a provision is introduced it might be advisable to integrate the provision on transparency obligations which is currently to be found in Article 52(2) AIA Proposal (see paragraph 3 above). There should also be a clarification that further requirements or restrictions following from other Titles of the Act or from other law remain unaffected (see paragraph 4 above).

Article 5b

Other use of biometric techniques

1. Biometric identification systems not covered by Article 5a, emotion recognition systems and biometric categorisation systems may be used only when such use is limited to what is strictly necessary for:

(a) the use for a specific purpose to which the affected persons have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;

(b) the use for purposes and under conditions referred to in Article 9 (2)(b), (c), (g), (h), (i) and (j) of Regulation (EU) 2016/679;

(c) the use for the purpose of law enforcement, migration, asylum or border control management in as far as purposes are proportionate to the aim pursued, respect the essence of the fundamental rights and interests affected and provide for suitable and specific measures to safeguard them.

2. **Emotion recognition systems and biometric categorisation systems may also be used where processing of the personal data of the natural person concerned is otherwise based on a legal ground under Regulation (EU) 2016/679 and the data are used exclusively for triggering a reaction that can, by its very nature, not have a negative impact on that natural person's legitimate interests and fundamental rights, and the data are erased or fully anonymised instantaneously without leaving any trace to the identifiable natural person.**

3. **Users of AI systems within the meaning of paragraph (1) shall inform of the operation of the system the natural persons exposed thereto unless this is inconsistent with the purpose within the meaning of paragraph (1) for which the system is used.**

4. **Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law, non-discrimination law and consumer protection law, remain unaffected.**

Although decision making will be addressed in more detail only in Part II of this Study, it is recommended to include, in the specific context of biometric techniques, a special rule on decision making based on biometric techniques. This rule would be without prejudice to Article 22 GDPR, but as the latter applies only to fully automated decisions without meaningful human intervention there is a conspicuous gap which should be filled. The proposed Article 5c combines elements of Article 22 GDPR and Article 14 (5) AIA Proposal but modifies the latter as it is problematic in several respects (see 6.4).

Article 5c

Decisions based on biometric techniques

1. **No action or decision which produces legal effects concerning the person exposed to biometric identification, emotion recognition or biometric categorisation, or which similarly significantly affects that person, is taken by the user on the basis of the output from the system unless this has been verified by means that are independent from the system and that provide a degree of reliability and accuracy appropriate to the significance of the action or decision. In particular, emotion recognition systems and biometric categorisation systems must, as such, not be used as legal evidence that the natural person concerned has in fact had the emotions, thoughts or intentions recognised by the system or belongs in fact to the category assigned by the system**

2. **Further requirements or restrictions following from other Titles of this Act or from other laws remain unaffected.**

List of high-risk AI systems in Annex III

It is recommended to extend the list in Annex III in several respects. First of all, Point 1 should be extended to biometric techniques in general and cover also emotion recognition systems where those systems are to be used for preparing decisions that may have legal effects or similarly significantly affect him or her (see 7.3.3.1). Minor amendments have also been suggested with regard to Point 4 in order to capture, e.g., social media harvesting in the employment context.

With regard to consumer interests, it is of utmost importance to add, in Point 5, a number of applications that imply a comparable fundamental rights risk as credit scoring does. These applications include individual risk assessment in the insurance context, customer rating according to complaint history and similar factors, and personalised pricing (see 7.3.2.2 and 7.3.2.3). With regard to the exception for small scale providers there should be a clarification that it includes only small scale providers who are at the same time the 'providers' (within the meaning of the AIA) of the relevant AI systems.

What is missing entirely in Annex III is AI systems intended for use by consumers. The AIA as it currently stands seems to assume that systems intended for consumers are covered by Article 6 (1) in conjunction with NLF

product safety legislation. However, this is not necessarily the case as NLF product safety legislation fails to cover a number of high-risk AI systems, or may not subject them to third-party conformity assessment (see 7.3.1). This is why it is recommended to insert a new area, which could be titled 'Use by vulnerable groups or in situations that imply vulnerability to fundamental rights risks' and that would include, for the time being, virtual assistants used for making important decisions (e.g. a shopping assistant, be it provided as a standalone digital service or embedded in devices such as a home assistant device or a smart fridge) and particular AI systems specifically intended for children (see above Point 5a).

ANNEX III

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric **techniques** ~~identification and categorisation of natural persons~~:
   - (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;
   - **(a) AI systems intended to be used for emotion recognition of natural persons where that recognition may lead to a decision that produces legal effects for the relevant natural person or similarly significantly affect him or her;**

5. 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.

6. Education and vocational training:
   - (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
   - (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

7. Employment, workers management and access to self-employment:
   - (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, **or for** evaluating candidates ~~in the course of interviews or tests;~~
   - (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

8. Access to and enjoyment of essential private services and public services and benefits, **including access to products:**
   - (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
   - (b) AI systems intended to be used
   - **(i)** to evaluate the creditworthiness of natural persons or establish their credit score,
   - **(ii) to evaluate the behaviour of natural persons such as with regard to complaints or the exercise of statutory or contractual rights in order to draw conclusions for their future access to private or public services,**
   - **(iii) for making individual risk assessments of natural persons in the context of access to essential private and public services, including insurance contracts, or**
   - **(iv) for personalised pricing within the meaning of Article 6 (1) (ea) of Directive 2011/83/EU,**

   with the exception of AI systems put into service by small scale providers

of AI systems for their own use;

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

5a. Use by vulnerable groups or in situations that imply vulnerability to fundamental rights risks
(a)AI systems intended to be used by children in a way that may seriously affect a child's personal development, such as by educating the child in a broad range of areas not limited to areas which parents or guardians can reasonably foresee at the time of the purchase;
(b)AI systems, such as virtual assistants, intended to be used by natural persons for taking decisions with regard to their private lives that have legal effects or similarly significantly affect the natural persons; […]

1.1.1 Title IV with a new focus on individual rights

In this study, it is recommended not to leave individual rights entirely to the GDPR, first, because it is not likely that the GDPR will be changed in the near future and the gaps filled (e.g. with regard to AI systems merely recommending action to a human) and, second, because AI-related individual rights are rather misplaced in the GDPR. The reason for the latter is that these individual rights are not focussed on the processing of input data relating specifically to the affected data subject but on the output data, which may have been generated with the help of (training etc.) data relating to very different data subjects, or with the help of non-personal data. This is why it is suggested to give Title IV of the AIA a new focus on individual rights in the context of AI systems that present either a transparency or a fairness risk (for details see 8.2.1), and also to rephrase the existing Article 52 on transparency obligations in the light o
f this new focus and clarify its application to social bots that merely generate content (see 8.2.2).

~~TRANSPARENCY~~ OBLIGATIONS FOR CERTAIN AI SYSTEMS POSING TRANSPARENCY OR FAIRNESS RISKS

Article 51a

Compliance with the obligations

1. This Title includes obligations for AI systems where one or both of the following conditions are fulfilled:
(a) use of the AI system involves a risk of confusion between AI system and humans, or their operations or activities, where such confusion might harm the legitimate interests of persons exposed to the AI system;
(b) use of the AI system leads to a decision with regard to a person that involves a material degree of evaluation or discretion and thus involves a fairness risk for the affected person.

2. The obligations of users of AI systems under this Title shall apply also to users who do not operate the AI system under their own authority but who solicit the services of another party using the AI system.

3. Providers of AI system whose intended use includes use within the meaning of paragraph 1 shall ensure that AI systems are designed and developed in such a way that users are able to comply with their obligations under this Title.

4. None of the provisions under this Title shall affect any prohibitions or restrictions for AI systems following from Title II or Title IIa or any requirements or obligations set out for high-risk AI systems in Title III of this Regulation.

Article 52

Transparency obligations for certain AI systems

1. Users of an AI system that interacts with natural persons ~~Providers~~ shall ensure ~~that AI systems intended to interact with natural persons are designed and developed in such a way~~ that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use~~. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.~~

2. **Users of an AI system that creates content or engages in [online] activities that are normally engaged in by natural persons ('bot') shall disclose that the content was created, or the [online] activities performed, by an AI system, unless the source of the content or [online] activities cannot reasonably be expected to matter to natural persons exposed thereto an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto.** ~~This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.~~

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.

3a. **Paragraphs 1, 2 and 3** ~~However, the first subparagraph~~ shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.

4. Paragraphs 1, 2 and 3 shall not **be read as legitimising the use of AI systems referred to beyond what is permitted by other law** ~~affect the requirements and obligations set out in Title III of this Regulation.~~

A central part of the revised Title IV should be two additional provisions that mirror and adapt Article 22 GDPR (right to scrutiny of individual decision-making, see 8.2.4) as well as the respective information duties in Articles 13 to 15 GDPR (right to explanation of individual decision-making, see 8.2.5) in a way tailored to the specific situation of AI-driven decision-making. Major benefits for affected persons would include that these individual rights do not only apply for fully automated decisions, but also to decisions recommended to humans, and that the right to receive an explanation would be much more explicit and include, in particular, the main parameters of decision-making and their relative weight as well as an easily understandable explanation of inferences drawn if the inference itself is a main parameter.

Article 52a

Scrutiny of individual decision-making

1. No decision which produces legal effects concerning a person, or which similarly significantly affects that person, is taken by the user on the basis of the output from an AI system unless the appropriateness and fairness of this decision has been verified by means that are appropriate to the nature and the significance of the decision and the role of the AI system in the decision-making process.

2. Unless otherwise specified by Union or Member State law, verification within the meaning of paragraph 1 may, in particular, consist in meaningful scrutiny, before the decision is taken,

by a natural person who is equipped with the appropriate
(a) abilities, training and decision-making authority;
(b) information with regard to the individual case; and
(c) safeguards against automation bias.

3. The user may replace ex-ante verification within the meaning of paragraphs 1 and 2 by equivalent other measures where the affected person has given explicit consent or where ex-ante verification is impossible or would cause unreasonable effort and is not strictly necessary for safeguarding the affected person's rights and freedoms and legitimate interests. Unless otherwise specified by Union or Member State law, such equivalent other measures may, in particular, consist in the right to
(a) obtain human intervention that satisfies the requirements under paragraph 2;
(b) provide additional information and express his or her point of view; and
(c) contest the decision with a meaningful chance of having it revised.

Article 52b

Explanation of individual decision-making

1. A decision which is taken by the user on the basis of the output from an AI system and which produces legal effects concerning a person, or which similarly significantly affects that person, shall be accompanied by a meaningful explanation of
(a) the role of the AI system in the decision-making process;
(b) the logic involved, the main parameters of decision-making, and their relative weight; and
(c) the input data relating to the affected person and each of the main parameters on the basis of which the decision was made.
For information on input data under point (c) to be meaningful it must include an easily understandable description of inferences drawn from other data if it is the inference that relates to a main parameter.

2. Paragraph 1 shall not apply to the use of AI systems
(a) that have only minor influence within the decision-making process;
(b) that are authorised by law to detect, prevent, investigate and prosecute criminal offences or other unlawful behaviour;
(c) for which exceptions from, or restrictions to, the obligation under paragraph 1 follow from Union or Member State law, which lays down appropriate other safeguards for the affected person's rights and freedoms and legitimate interests; or
(d) where the affected person has given explicit consent not to receive an explanation.

3. The explanation within the meaning of paragraph 1 shall be provided at the time when the decision is communicated to the affected person. However, the user may provide the explanation only at a later point upon the affected person's request, where providing the explanation immediately is not strictly necessary for safeguarding the affected person's rights and freedoms and legitimate interests, in which case the user shall inform the affected person of the right under this Article and how it can be exercised.

1.1.2 Liability

Liability for AI systems should not primarily be dealt with in the AIA itself, but be largely a matter for product liability law, national tort law and/or a new EU regime of AI liability. However, as these liability regimes are not well suited to address harm caused by fundamental rights risks, it is advisable to insert two provisions in the AIA itself, one on vicarious liability (see 9.3.2) and one on liability for lack of 'fundamental rights safety' (see 9.3.3). The former would help overcome existing uncertainties with regard to vicarious liability under national law (such as §§ 1313a, 1315 ABGB or §§ 278, 831 BGB), the latter would increase legal certainty (including concerning compensation of non-economic loss) with regard to doctrines such as Schutzgesetzverletzung (cf. § 1311 ABGB or § 823 (2) BGB).

Article 72a

Vicarious liability for AI systems

1. **A user of an AI system shall be liable for harm caused by any lack of accuracy or other shortcoming in the operation of the system to the same extent as that user would be liable for the acts or omissions of a human employee mandated with the same task as the AI system.**

2. **Where a human employee would not have been able to fulfil the task fulfilled by the AI system (such as where the task requires computing capabilities exceeding those of humans) the point of reference for determining the required level of performance is available comparable technology which the user could be expected to use.**

Article 72b

Right to compensation and liability

1. **Where non-compliance of a party with any obligations following from Titles II, IIa, III or IV of this Regulation has resulted in an increased risk for the safety or fundamental rights of a person, and where that person has suffered economic or non-economic harm [Opt: material or non-material damage] because the risk has materialised, the person shall have the right to receive compensation from the party who failed to comply with its obligations.**

2. **Where a high-risk AI system fails to comply with the requirements set out in Articles 13 to 15 and the harm suffered is of a kind typically resulting from such non-compliance there shall, for the purposes of liability under paragraph 1, be a presumption that the non-compliance has caused the harm.**

3. **A party who has failed to comply with its obligations shall be exempt from liability under paragraph 1 if it proves that it is not in any way responsible for the non-compliance.**

4. **Where more than one party has failed to comply with their obligations and is liable under paragraph 1, each party shall be held liable for the entire damage in order to ensure effective compensation of the affected person. Where a party has paid full compensation for the damage suffered that party shall be entitled to claim back from the other liable parties that part of the compensation corresponding to their part of responsibility for the damage.**

1.1.3 Enforcement

In addition to including the AIA, or the relevant provisions thereof, in the list of legal instruments in Annex I to the Representative Actions Directive (RAD) (see 10.1.2), it is recommended to include a new enforcement mechanism with regard to systemic risks (for details see 10.2.2). Systemic risks may arise, in particular, where a high-risk AI system that complies with the AIA has, in the light of its significant market coverage, the potential of changing our societies and economies, causing characteristic features and smaller deficiencies (that may be acceptable in an AI system when seen in isolation) to become a systemic risk. For example, bias in a system that is dominant on the relevant market could cause new disadvantaged groups to emerge that can no longer be captured by non-discrimination law as it currently exists, or widespread use of an AI system could have detrimental effects on human skills and competences. The new enforcement mechanism suggested has been inspired by Articles 25 ff DSA, and it includes data access for vetted researchers.

CHAPTER 2A

ADDITIONAL OBLIGATIONS FOR VERY LARGE PROVIDERS TO MANAGE SYSTEMIC RISKS

Article 62a

Very large providers

1. This Chapter shall apply to providers of high-risk AI systems listed in Annex III for which both of the following conditions are fulfilled:

(a) the provider has a share of [...] percent or above in the market for AI systems of the relevant type, considering the AI system's core functionalities, with regard to the whole Union, or a share of [...] percent or above in the relevant market in at least three Member States; and

(b) [...] percent or above of decision-making of the relevant kind listed in Annex III significantly relies on the use of that type of AI system.

When calculating the share within the meaning of point (a), AI systems that are not placed on the market or put into service under the provider's own name or trademark, but that use the provider's AI system as a basis or component in a way that significantly influences any systemic risks presented by those AI systems, shall be included.

2. The Commission shall adopt delegated acts in accordance with Articles 73 and 74, after consulting the Board, to lay down a specific methodology for calculating the market share referred to in paragraph 1. In those delegated acts, the Commission may also define different percentages than referred to in paragraph 1 for particular high-risk AI systems where there is reason to believe that systemic risks resulting from that type of AI system are significantly higher or lower than for other AI systems listed in Annex III.

3. The Board shall verify, at least once a year, whether the market shares of providers whose AI systems are used in the Union is equal to or higher than the shares referred to in paragraphs 1 and 2. On the basis of that verification, it shall adopt a decision designating the provider as a very large provider for the purposes of this Regulation, or terminating that designation, and communicate that decision, without undue delay, to the provider concerned and to the Commission.

4. The Commission shall ensure that the list of designated very large providers is published in the Official Journal of the European Union and keep that list updated. The obligations of this Chapter shall apply, or cease to apply, to the very large providers concerned from four months after that publication.

Article 62b

Systemic risk assessment

1. As part of the quality management system referred to in Article 17 and post-market monitoring system referred to in Article 61, very large providers shall identify, analyse and assess, at least once a year, any significant systemic risks stemming from the functioning and use made of the AI systems provided by them in the Union.

2. This risk assessment shall be specific to the AI systems they provide and shall, in any case, include the following systemic risks:

(a) any negative effects for the exercise of fundamental rights, for example respect

for private and family life, data protection, the prohibition of discrimination, the rights of the child and access to an effective remedy and a fair trial, as enshrined in Articles 7, 8, 21, 24 and 47 of the Charter respectively;

(b) any negative effects for democracy, the rule of law, the functioning of state institutions, the stability of societies and economies, protection of the environment and the combat against climate change, and other important public interests;

(c) any risks resulting from uniformity of decision-making, including for the emergence of new disadvantaged groups, the reduction of diversity in affected groups (e.g. recruited individuals), and a steering function for human behaviour as affected individuals adapt their behaviour to the parameters relied on by the AI system;

(d) any risks resulting from a reduction in human skills and competences, including for the ability to detect and correct errors and to act independently of the AI system where the system is unavailable;

(e) risks of intentional manipulation of their AI system, including by means of targeted inauthentic behaviour of affected persons, malicious interferene by third parites, or hybrid warfare, with an actual or foreseeable negative effect on important public or private interests.

Article 62c

Mitigation of systemic risks

1. Very large providers shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 62b. Such measures may include, where applicable:

(a) adapting AI systems, their decision-making processes, their features or functioning, or the instructions and specificaitons accompanying them;

(b) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;

(c) …

2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:

(a) identification and assessment of the most prominent and recurrent systemic risks reported by very large providers or identified through other information sources;

(b) best practices for very large providers to mitigate the systemic risks identified.

3. The Commission, in cooperation with the Board, may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations.

Article 62d

Independent audit

1. Very large providers shall be subject, at their own expense and at least once a year, to audits to assess compliance with the following:

(a) the obligations set out in Chapter 3 of Title III;

(b) any commitments undertaken pursuant to the codes of conduct referred to in Article 69.

2. Audits performed pursuant to paragraph 1 shall be performed by organisations which:

(a) are independent from the very large providers concerned;

(b) have proven expertise in the area of risk management, technical competence and capabilities;

(c) have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards.

3. The organisations that perform the audits shall establish an audit report for each audit. The report shall be in writing and include at least the following:

(a) the name, address and the point of contact of the very large provider subject to the audit and the period covered;
(b) the name and address of the organisation performing the audit;
(c) a description of the specific elements audited, and the methodology applied;
(d) a description of the main findings drawn from the audit;
(e) an audit opinion on whether the very large provider subject to the audit complied with the obligations and with the commitments referred to in paragraph 1, either positive, positive with comments or negative;
(f) where the audit opinion is not positive, operational recommendations on specific measures to achieve compliance.

4. Very large providers receiving an audit report that is not positive shall take due account of any operational recommendations addressed to them with a view to take the necessary measures to implement them. They shall, within one month from receiving those recommendations, adopt an audit implementation report setting out those measures Where they do not implement the operational recommendations, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures they may have taken to address any instances of non-compliance identified.

Article 62e

Transparency reporting obligations for very large providers

1. Very large providers shall make publicly available and transmit to the Board and the Commission, at least once a year and within 30 days following the adoption of the audit implementing report provided for in Article 62d(4):

(a) a report setting out the results of the risk assessment pursuant to Article 62b;
(b) the related risk mitigation measures identified and implemented pursuant to Article 62c;
(c) the audit report provided for in Article 62d(3);
(d) the audit implementation report provided for in Article 62d(4).

3. Where a very large provider considers that the publication of information pursuant to paragraph 2 may result in the disclosure of confidential information of that provider or of the users of the AI system, may cause significant vulnerabilities for the security of its AI system, may undermine public security or may harm users or affected individuals, the provider may remove such information from the reports. In that case, that provider shall transmit the complete reports to the Board and the Commission, accompanied by a statement of the reasons for removing the information from the public reports.

Article 62f

Data access and scrutiny by vetted researchers

1. Upon a reasoned request from the Commisison, very large providers shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 3 of this Article, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union as set out in Article 62b(1), including as regards the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 62c. In making a request, the Commission shall take due account of the rights and interests of the providers and users of the AI system concerned, including the protection of personal data, the protection of confidential information, in particular trade secrets, and maintaining the security of their AI systems.

2. Very large providers shall facilitate and provide access to data pursuant to paragraph 1 through appropriate interfaces specified in the request, including online databases or application programming interfaces.

3. Upon a duly substantiated application from researchers, the Commission shall award them the status of vetted researchers and issue data access requests pursuant to paragraph 1, where the researchers demonstrate that they meet all of the following conditions:

(a) they are affiliated to a research organisation as defined in Article 2 (1) of Directive (EU) 2019/790 of the European Parliament and of the Council;

(b) they are independent from commercial interests;

(c) they are in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and they describe in their request the appropriate technical and organisational measures they put in place to this end;

(d) the application submitted by the researchers justifies the necessity and proportionality for the purpose of their research of the data requested and the timeframes within which they request access to the data, and they demonstrate the contribution of the expected research results to the purposes laid down in paragraph 1;

(e) the planned research activities will be carried out for the purposes laid down in paragraph 1;

(f) they carry their activities according to the procedures laid down in delegated acts referred to in paragraph 7;

(g) they have not already filed the same application with the Commission.

4. The Commission shall issue a decision terminating the access if it determines, following an investigation either on its own initiative or on the basis information received from third parties, that the vetted researcher no longer meets the conditions set out in paragraph 3. Before terminating the access, the Commission shall allow the vetted researcher to react to the findings of its investigation and its intention to terminate the access.

5. Upon completion of the research envisaged in paragraph 1, the vetted researchers shall make their research results available to the Commission free of charge. The Commission may make the research results publicly available, taking due account of the rights and interests of the providers and users of the AI system concerned, including the protection of personal data, the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

6. The Commission shall, after consulting the Board, adopt delegated acts laying down the technical conditions under which providers of very large providers are to share data pursuant to paragraphs 1 and 2 and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions and relevant objective indicators, as well as

procedures under which such sharing of data with vetted researchers can take place in compliance with Regulation (EU) 2016/679, taking into account the rights and interests of the providers and users of the AI system concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their AI system.

In addition to a new enforcement mechanism for systemic risks it is suggested to insert a provision that avoids threats to public and national security interests (see 10.3) which could result if national authorities in all 27 Member States had full access to all relevant data and the source code of, e.g., AI systems that are safety components in critical infrastructure (such as AI systems used to detect attacks on power grids within the Union).

Article 70a

Exceptions for AI systems with enhanced confidentiality requirements

1. **A provider of a high-risk AI system that is confronted with a request by a competent national authority for information, documentation, access to data, disclosure of the source code or a similar measure under this Regulation may refuse to comply with the request if that provider can demonstrate that the relevant materials would, if disclosed to unauthorised parties, jeopardise public and national security interests.**

2. **A provider relying on paragraph 1 shall immediately notify the Commission of the refusal to comply with the request and the reasons of the refusal. The Commission shall, upon having investigated the matter, issue a decision addressed at the relevant national authority and the provider. In that decision, the Commission may provide that only Commission staff holding the appropriate level of security clearance shall be allowed to access the relevant**

AK EUROPA

The Austrian Federal Chamber of Labour is by law representing the interests of about 3.8 million employees and consumers in Austria.
The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.