DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Committees on Labour Law, Surveillance, Intellectual Property, European Affairs, IT Law and Migration Law

on the Proposal of the European Comission 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, adopted on 21 April 2021 (COM (2021) 206 final)

Position Paper No.: 57/2021 Berlin/Brussels, November 2021

Members of the Committee on Labour Law

- Rechtsanwältin Dr. Nathalie Oberthür, Köln (Chair and Rapporteur)
- Rechtsanwalt Dr. Christian Arnold, Stuttgart
- Rechtsanwältin Regina Bell, München
- Rechtsanwältin Dr. Susanne Clemenz, Gütersloh
- Rechtsanwalt Prof. Dr. Björn Gaul, Köln (Rapporteur)
- Rechtsanwalt Roland Gross, Leipzig
- Rechtsanwalt Jürgen Markowski, Offenburg
- Rechtsanwalt Benja Mausner, Stuttgart
- Rechtsanwalt Dr. Thomas Müller-Bonanni, Düsseldorf
- Rechtsanwältin Dr. Barbara Reinhard, Frankfurt am Main
- Rechtsanwältin Dr. Ulrike Schweibert, Frankfurt
- Rechtsanwalt Dr. Uwe Silberberger, Düsseldorf

In charge in the Berlin office

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Members of the Committee on Surveillance

- Rechtsanwältin Lea Voigt, Bremen (Chair)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (Rapporteur)
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (permanent guest)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Prof. Dr. Mark A. Zöller, München (permanent guest)

In charge in the Berlin office

- Rechtsanwalt Max Gröning

Members of the Committee on Intellectual Property

- Rechtsanwalt Prof. Dr. Jochen Bühling, Düsseldorf (Chair and Rapporteur)
- Rechtsanwältin Jana Bogatz, München
- Rechtsanwalt Dr. Dirk Bruhn, Hamburg
- Rechtsanwalt Klaus Haft, Dipl.-Phys., Düsseldorf
- Rechtsanwältin Dr. Verena Hoene, Köln
- Rechtsanwalt Prof. Dr. Reinhard Ingerl, LL.M., München
- Rechtsanwältin Dr. Andrea Jaeger-Lenz, Hamburg
- Rechtsanwalt beim Bundesgerichtshof Dr. Matthias Koch LL.M., Karlsruhe
- Rechtsanwalt Prof. Dr. Johannes Kreile, München
- Rechtsanwalt Dr. Henrik Lehment, Düsseldorf
- Rechtsanwältin Dr. Birte Lorenzen, Hamburg

In charge in the Brussels office

- Hannah Adzakpa, LL.M.

Members of the Committee on European Affairs

- Rechtsanwältin Dr. Claudia Seibel, Frankfurt (Chair)
- Rechtsanwältin Béatrice Deshayes, Paris
- Rechtsanwalt Prof. Dr. Christian Duve, Frankfurt am Main (Rapporteur)
- Rechtsanwalt Prof. Dr. Thomas Gasteyer, LL.M., Frankfurt am Main
- Rechtsanwalt Prof. Dr. Hans-Jürgen Hellwig, Frankfurt am Main
- Rechtsanwalt Dr. Ulrich Karpenstein, Berlin
- Rechtsanwältin Gül Pinar, Hamburg

- Rechtsanwalt Prof. Dr. Dirk Uwer, Düsseldorf
- Rechtsanwalt Michael Jürgen Werner, Brüssel

In charge in the Brussels office

- Hannah Adzakpa, LL.M.

Members of the Committee on IT Law

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Chair)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg (Rapporteur)
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

In charge in the Berlin office

- Rechtsanwältin Nicole Narewski

Members of the Committee on Migration Law

- Rechtsanwältin Gisela Seidler, München (Chair)
- Rechtsanwalt Dr. Marco Bruns, Frankfurt am Main, stellvertretender Vorsitzender
- Rechtsanwalt Dr. Wolfgang Breidenbach, Halle/Saale
- Rechtsanwältin Maria Kalin, Ulm
- Rechtsanwalt Tim W. Kliebe, Frankfurt am Main
- Rechtsanwalt Dr. Jonathan Leuschner, Frankfurt am Main
- Rechtsanwältin Kerstin Müller, Köln
- Rechtsanwalt Berthold Münch, Heidelberg
- Rechtsanwalt Thomas Oberhäuser, Ulm
- Rechtsanwältin Simone Rapp, Berlin
- Rechtsanwalt Rolf Stahmann, Berlin (Rapporteur)
- Rechtsanwältin Eva Steffen, Köln
- Rechtsanwalt Christoph Tometten, Berlin

In charge in the Berlin office

- Rechtsanwältin Bettina Bachmann

Mailing List:

Germany

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Ausschuss für die Angelegenheiten der Europäischen Union
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
Justizministerien und -senatsverwaltungen der Länder
Rechtsausschüsse der Landtage
Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
Stiftung neue Verantwortung e.V.
DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende der DAV-Landesverbände
Vorsitzender des FORUMs Junge Anwaltschaft

Europe

European Commission
- Directorate-General for Justice and Consumers
- Directorate-General for Communications Networks, Content and Technology

European Parliament
- Committee on the Internal Market and Consumer Protection
- Committee on Legal Affairs
- Special committee on artificial intelligence in a Digital Age

The Council of the European Union
Permanent Representation of the Federal Republic of Germany to the EU
Legal Advisers of the Permanent Representations of the German Bundesländer to the EU
Council of Bars and Law Societies of Europe (CCBE)
Vertreter der Freien Berufe in Brüssel
DIHK Brussels
BDI Brussels

Press:

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion heise online
JurPC

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 61.000 German lawyers and lawyer-notaries in 252 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level.

---

1. Summary

The German Bar Association (DAV) welcomes the EU Commission's proposal for a regulation laying down harmonised rules on Artificial Intelligence and amending certain EU legislative acts (hereafter abbreviated as “AIA Proposal”). The intention behind the AIA Proposal is to promote innovation and create legal certainty by regulating AI in a harmonized and minimally invasive way.

The DAV has responded to the Commission’s White Paper on AI in Position Paper No. 40/2020. In this Position Paper, the DAV has already advocated for fully respecting fundamental rights in the context of AI. The function of the legal profession as representatives of citizens, acting in a personal and fully confidential manner, must be protected. The DAV has also continuously pointed the particularly high fundamental rights risks when using AI systems in the judiciary. This is why the use of AI systems in the judiciary requires very strict rules that correspond to these fundamental right risks. Judicial and similarly binding decisions by state actors must never be fully automatic. In addition, effective redress and control mechanisms must be created for those whose rights are affected by AI. The need to preserve the primacy of human decision-making in the judiciary and public authorities is also at the forefront of the Council of Bars and Law Societies of Europe (CCBE) Position Paper on the AIA Proposal. The DAV participated in the drafting of the opinion and supports the main positions expressed therein.

When providing a first feedback to the AIA Proposal, the DAV pointed out, among other things, that the complexity, length and numerous references of the AIA Proposal to other regulations and directives could lead to practical application difficulties and legal uncertainties. Hence, the aim of this position paper is to support the negotiations in the EU Parliament and Council by summarizing and synchronising the DAV’s previous statements and adding additional points, as necessary.

2. Definition, Scope and General Dogmatics

2.1 Definition of AI systems

In light of the AIA Proposal's various, sometimes far-reaching legal consequences; the definition of AI systems is of essential relevance. The AIA Proposal legally defines AI systems in Art. 3 (1). This definition appears to be too narrow with regard to future developments, as it refers to human-defined objectives. However, it is entirely possible that AI systems themselves might define goals in the future. This scenario is possible when approach the so-called "strong" AI. In this respect, a definition which takes strong AI into account will be necessary sooner or later.

At this point in time, there is an immediate need for improvement regarding Annex I of the AIA Proposal. Annex I defines AI systems that fall under the scope of the AI proposal very widely. In the current wording, normal expert systems or search and optimization methods would also fall within the AIA Proposal's scope.

One possible restriction could be to define AI systems under Annex I as only comprising those systems whose decisions or behaviour are to be regarded as practically unpredictable (by reasonable means). This way, it could be avoided that numerous, already existing IT systems or software solutions are subjected unnecessarily to the extensive regulation for AI systems planned by the Commission.

2.2 Scope of Application

The DAV welcomes the horizontal nature of the AIA Proposal. Art. 2 (2) of the AIA Proposal practically completely excludes the vehicle and aviation industries the scope of application, by referencing the corresponding Regulations. A corresponding Regulation which includes the vehicle and aviation industries should be proposed promptly, as is already planned by the Commission.

2.3 Regulatory Technique, Scope and Structure

The DAV welcomes the risk-based approach of the AIA Proposal. In its Position Paper on the White Paper, the DAV has advocated for a differentiation according to at least five risk levels. Under this approach, all AI systems would have to meet certain

transparency, security and control requirements, depending on the intensity of their intervention. However, the binary classification into high-risk / non-high-risk AI systems - as is envisaged in the AIA Proposal - leaves less room for differentiation of other risk levels. Should the AIA Proposal be revised in this respect, a further development of more risk-levels would be conceivable.

It could also be helpful to reduce some of the complexity, which is inherent in the AIA Proposal. One reason for the perceived complexity is due to the numerous cross-references. In particular the cross-references to other Regulations (e.g. Art. 42(2) and Art. 47 (6) AIA Proposal) make the AIA Proposal difficult to read and hence more difficult to apply.

3. Prohibited AI Systems

Art. 5 AIA Proposal lists *intolerable and prohibited* AI systems. This Article intends to prevent particularly serious violations of fundamental or human rights. The AI systems listed in Art. 5 (1) AIA Proposal are indeed problematic, which is why the DAV does not object to this list. What is missing, however, is a provision that creates certain guidelines to provide the basis for a future expansion this list. In other words, what is needed are clear criteria that help to distinguish between AI systems that are prohibited and AI systems that are permitted. Additionally, in terms of fundamental rights relevance, a clearer distinction should be made between the use of AI by the state on the one hand, and by private parties on the other hand.

3.1 Social Scoring

According to Art. 5 (1) (c) AIA Proposal, certain AI systems used by public authorities or on their behalf and intended “for the evaluation or classification of the trustworthiness of natural persons” are prohibited (so-called “Social Scoring”). Due to the intensity of intervention and the particular risks of social scoring, the DAV welcomes this prohibition. Therefore, it is regrettable that the prohibition is softened by the conditions mentioned in (i) and (ii). The wording of the conditions leaves so much room for a broad interpretation that the prohibition could be circumvented. In particular, the phrase "unrelated to the contexts" (i), as well as the terms "unjustified or disproportionate" (ii), could lead to an overly broad interpretation which might circumvent the prohibition. Furthermore, the prohibition of Social Scoring should be extended to private actors and not be limited to public authorities. In this context, the DAV draws attention to the CCBE

Position Paper, which points out the dangers of Social Scoring with regards to democracy and the rule of law. Social Scoring does not only violate the rights to privacy and family life, but also exacerbates the risk of discrimination. Anonymity, including not being scored for certain behaviours, is often the cornerstone of being able to fully exercise one's fundamental rights. This right to anonymity and privacy is eroded or even made impossible by Social Scoring. In a worst case scenario, Social Scoring could even *de facto* suspend the presumption of innocence.

Proposed amendment to Art. 5

(1) The following artificial intelligence practices shall be prohibited:
(...)
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;~~
(…)

3.2 Biometric Remote Identification

Art. 5 (1) (d) AIA Proposal prohibits the use of real-time biometric remote identification systems in publicly accessible spaces for law enforcement purposes. However, there are three broad exceptions to this prohibition. The DAV criticizes that the ban on biometric identification systems only applies to real time-situations, whereas otherwise the same systems are only classified as high-risk AI systems. It is not apparent that the dangers of such systems are so different as to justify this different treatment. Moreover, Art. 5 AIA Proposal only prohibits biometric identification systems when used for law enforcement purposes, hence allowing the use by private actors.

Many studies demonstrate the high-risks of biometric identification systems. The likelihood of serious violations of fundamental rights such as the right to privacy or the principle of non-discrimination is very high and can have far-reaching consequences for the individuals concerned.[1] In many situations, anonymity is the most important

[1] Christiane Wendehorst & Yannic Duller, Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their

protection of freedom, with and biometric identification technologies covering large areas of public space threatening this freedom. Biometric identification systems also appear to be prone to high error rates and vulnerable to manipulation. Therefore, the DAV supports the Joint Opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) of June 2021, which calls for a general ban of biometric surveillance in public spaces.[2] A recent EU Parliament Resolution argues along the same lines.[3] The use of remote biometric identification systems in publicly accessible spaces should be completely banned - regardless of whether the surveillance is carried out by private or state actors and regardless of whether it takes place in real time or with a delay.

Proposed amendment to Art. 5

(1) The following artificial intelligence practices shall be prohibited:
(….)
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 the life or physical safety of natural persons or of a terrorist attack;~~

~~(iii) the detection, tracing, identification or prosecution of a perpetrator or suspect of an offense, as defined in Article 2(2) of Council Framework Decision 2002/584/JHA62 , which is punishable under the law of the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years.~~

3.3 Absence of a Ban on "Robot-Judges"

Art. 5 AIA Proposal does not currently provide for a general ban on AI systems that take independent judicial decisions. However, as already explained in detail in SN 40/2020 (paras. 22-31), judicial and similarly binding decisions by state actors may not be fully automated.

No AI system can fulfil the individual's right to be heard by an impartial and independent tribunal, as stipulated in Art. 47 (2) EU Charter of Fundamental Rights. It is often impossible to determine on which criteria an AI system bases its results. At the same

current and future use in public spaces, Study Requested by the JURI and PETI committees, August 2021; Studie Greens/EFA: current practices of biometric mass surveillance in the EU, 25 Oct 2021.

[2] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, RN 29-35.

[3] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI).

time it is often impossible to find out on which - possibly insufficient or biased - information on the facts and case law the AI system has been trained. Hence, the verification of the impartiality of any AI system is likely to be practically impossible in many constellations. Moreover, the criterion of impartiality also requires that the judge who takes the decision can be identified as an actor. However, AI systems do not have legal personality and therefore cannot be held responsible for a decision. Therefore, the substation of AI systems AI for a human, judicial decision would constitute a violation of the right to be heard by an independent and impartial court.

Proposed addition to Art. 5
(1) The following artificial intelligence practices shall be prohibited: (….) ***e) the placing on the market, putting into service, or use of AI systems that are aimed at automating judicial and similarly intrusive binding decisions by state actors.***

3.4 Absence of a Ban on Predictive Policing Violates the Presumption of Innocence

According to Annex III.6 (a) AIA Proposal, AI systems that are “intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences” are classified as high-risk AI systems.

The DAV demands that any kind of so-called "predictive policing" must be prohibited, both in the area of law enforcement and in the area of surveillance. AI systems intended for the purpose of predictive policing can be used in criminal proceedings to create individual assessments for the risk of re-offending. These can be used to determine the duration of a convicted person's imprisonment, for example. In the area of surveillance, police authorities already make use of AI-supported predictive policing to create location-based danger forecasts. Extending such automated forecasts to the behaviour of individual persons in order to estimate the probability of future dangerous actions by the persons concerned should be prohibited.

The use of AI systems for the purposes of predictive policing in law enforcement violates the right to a fair trial. Using them to make individualized predictions of perceived danger prognosis in surveillance would create an unacceptable risk of

discrimination against certain groups of the population. AI systems used for predictive policing reflect biases in data sets. These biases stem from the fact that traditional crime statistics reflect police activities. Since police activity is more prevalent with some social groups than other groups, this imbalance is incorporated into the datasets. Any predictive policing AI systems built on such datasets thus reflects police bias. This means that predictive policing AI systems used in law enforcement violate the presumption of innocence by treating individuals as potential suspects, solely based on inferences about a larger group. The results of these risk assessment tools in the criminal justice system and in pre-trial contexts, such as using algorithms to profile individuals in legal proceedings, pose a serious threat to fundamental rights. The same applies to individual behavioural predictions in the field of surveillance.

It must always be taken into account that AI systems are based on purely mathematical algorithms, which are exclusively based on statistical calculations (forecasts, probabilities, correlations) with all the associated sources of errors known in statistics. The system is only as good as the quality of the input-data, which is given to learn the "correct" probability algorithm. In addition, the way algorithms work is neither transparent nor explainable. This is the famous black box-problem: “*We know what information is fed in and what comes out, but what happens in between is a 'black box*'”.[4] Consequently, decisions taken on the basis of such "findings" calculated by machines might lead to a paradoxical "reversal of the burden of proof" for the person who is affected by those “findings” in criminal proceedings. It is up to the affected person to prove (in view of the "black box") that he or she has been unjustly incriminated by a machine algorithm.

These tools base their assessments on a comprehensive collection of personal data that need have nothing to do with a subject's alleged misconduct. In addition, some predictive policing AI systems may also take into account the number of times a person has been suspected of a crime, whether or not that person has subsequently been convicted.

This collection of personal data for the purpose of predicting the risk of re-offense cannot be considered necessary or proportionate to the objective pursued, particularly

[4] See for example Billis, Knust, Rui, FS for Sieber, pp. 693 ff/707, with further references.

in light of the impact on the right to privacy and the presumption of innocence. A report by Fair Trials shows that the introduction of AI systems for predictive policing has led to discriminatory outcomes in many EU member states.[5]

The use of AI systems presents challenges in the area of digital forensics and risk assessments for re-offending, since the specific functioning of the algorithms is not usually disclosed to the individuals affected by the results of their application. As a result, the affected person cannot challenge the predictions made by the algorithms, which jeopardizes the right to a fair trial. Since the AIA Proposal does not provide for sufficient transparency obligations which would make the precise functioning of the algorithmic system publicly available to users in a reasonable manner, there is no possibility to challenge a decision, which would be taken based on this data.

Even if the information required for this were freely available, the parties concerned would have to bear the costly and time-consuming burden of data analysis themselves. Such a burden would significantly worsen their situation in the proceedings and violate the principles of a fair trial.

Proposed addition to Art. 5
(1) The following artificial intelligence practices shall be prohibited: (…) ***(f) AI systems to be used by law enforcement and security agencies for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offenses;*** (…)

3.5 Absence of a Ban on Polygraphs for Law Enforcement and in Migration Law

Annex III.6 (b) AIA Proposal classifies those AI systems as high-risk that are "intended to be used by law enforcement authorities as polygraphs". According to Annex III.7 (a), under the heading of "Migration, asylum and border control management", those AI systems that are "intended to be used by competent public authorities as polygraphs" are classified as high-risk. Since the reliability of polygraphs is highly controversial and due the great risks with regard to the presumption of innocence and general defence

[5] Fair Trials: "*Automating injustice: the use of Artificial intelligence & Automated decision-making systems in Criminal justice in Europe*", 9 September 2021.

rights, the DAV advocates for a complete ban on polygraphs, including a ban on their use by private actors.

Proposed amendment to Art. 5
(1) The following artificial intelligence practices shall be prohibited: (...) ***(g) AI systems intended to be used as polygraphs and similar tools to detect the emotional state of a natural person;*** (…)

3.5 Absence of a Ban on AI Systems in the Area of Migration, Asylum and Border Control Management

The DAV joins the CCBE Position Paper in its call for a ban on AI systems in the area of migration, asylum and border control management, until they have been independently assessed for compliance with international human rights standards. There are more and more examples of the use of AI systems in the field of migration control, which pose a growing threat to the fundamental rights of migrants, EU law and human dignity.

EU migration policies are increasingly supported by AI systems such as facial recognition, profiling, and predictive tools used in migration management processes, including forced return. Hence, there is a high risk that these areas of application may violate the right to privacy, the right to non-discrimination and various principles of international migration law, including the right to asylum. In particular, there is also a significant imbalance of power that is exacerbated and exploited by the use of AI systems in the area of migration, asylum, and border control management.

In migration law, many decisions taken by the authorities are influenced by a large number of complex factual circumstances in specific individual cases. Very often, an evaluation and detailed weighing of various circumstances is required in this context. Additionally, the requirement that a decision must be proportional is extremely important. In many cases, the authorities also have discretionary powers. At most, the use of AI systems that are classified as high-risk would be conceivable in areas in which evaluations or considerations of the facts and legal consequences do not play a role.

The DAV is particularly critical about the follow scenarios:

- AI systems that assess the credibility of factual information or the credibility of applicants themselves in asylum procedures, as well as the assessment of persecution risks in the country of origin;
- AI systems that evaluate of the coherence of an intended purpose of stay, including possible risks of abuse in visa procedures;
- AI systems that evaluate the existence of a family relationship which is deemed worthy of legal protection in family reunification procedures or with regard to the protection of marriage and family under immigration law;
- AI systems that evaluate required professional and academic qualifications in the field of immigration law;
- AI systems that assess the potential dangers posed by a foreigner to public safety and order in the laws applicable to deportation,
- AI systems that evaluate the risks of escape in cases of detention pending deportation.

Proposed amendment to Art. 5

(1) The following artificial intelligence practices shall be prohibited:

(…)

(h) In the area of migration, asylum and border control, the following practices are prohibited until they have been independently assessed for compliance with international human rights standards:

(i) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, an risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(ii) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(iii) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

4. High-Risk AI Systems

The classification rules for high-risk AI systems are legally defined in Art. 6 ff. AIA Proposal. This definition is convincing to the extent that it regulates safety-related AI or AI-based products (Art. 6 (1) AIA Proposal). Yet whether the regulated systems should really be limited to those for which third-party conformity testing is required should be

critically questioned. At the same time, however, the principle of risk-appropriate regulation of AI systems should be retained, and only those systems whose characteristics make increased regulation necessary should be classified as high-risk AI systems. After all, the list of EU legislation as contained in Annex II should clearly point towards a potential higher risk. Against this background, it is understandable that Art. 6 (2) AIA proposal provides for the possibility of classification as a high-risk AI system – and hereby a highly regulated AI system – by virtue of Annex III.

Yet, the categories of high-risk AI systems listed in Annex III are too broad. AI systems do not require ex ante regulation in the form of transparency obligations or specific requirements for the data base, if regulatory objectives can be achieved via principles of the free market-economy. As an example, the online language programme "Duolingo" currently falls under the scope of Annex III. This company offers an AI-based language test which university applicants can use as proof of their foreign language skills.[6] A commercial test system that erroneously or without comprehensible reason withholds a successful test result from participants will not prevail against other test systems available on the market. The providers of such applications have a vested interest in offering comprehensible and high-quality tests. Hence, an additional ex ante regulation is superfluous in this context.

Additionally, even if the Commission is primarily concerned with regulating AI systems that are relevant to fundamental or human rights, the criteria for inclusion in the list of Annex III are not immediately obvious. Hence, it is difficult to assess the possibilities how Annex III might be expanded on in the future, in accordance with Art. 7 AIA Proposal. For this reason, Art. 7 (2) AIA Proposal should provide even clearer guidance under which principles AI systems could be included in Annex III in the future.

The DAV assesses the main principles for high-risk AI systems as envisaged by the AIA Proposal positively, in particular:

- Strong obligations for quality and risk management (Arts. 9, 17 AIA Proposal), including post-market monitoring (Art. 61 AIA Proposal);
- Strong regulation of training and testing data (Art. 9 (5), (6), (7) and Art. 10 AIA Proposal);

[6] https://www.ft.com/content/a5970b6c-e731-45a7-b75b-721e90e32e1c, 25 July 2021.

- The requirement to implement the possibility of an automatic recording of events, so-called event “logs” (Art. 12, 16 (a), (d); resp. Art. 29 (5) AIA Proposal);
- Monitoring obligations not only for the provider, but also for the user (Art. 29 (4) AIA Proposal).

These requirements and obligations should result in being able to counteract to a certain extent the typical risks associated with AI systems. This should hold true at least when it comes to the so-called weak AI - in particular those AI systems that act in a self-learning manner to a certain degree.

There is one particular difficulty when trying to regulate AI systems. On the one hand, AI systems can substitute or even take over human behaviour and human decisions, which promotes efficiency. On the other hand, AI systems’ behaviour and decisions are often *unpredictable*, which corresponds to a higher requirement for quality and risk management. Additionally, deficiencies of AI systems tend to not only be based on design and fabrication, but can also stem from the training of the systems (e.g. neural networks). In this respect, the requirements for training and governance of training and other data presumably have a risk-reducing effect (e.g. Art. 9 (5), (6), (7) and Art. 10 AIA Proposal). However, since wrong decisions and misconduct of AI systems cannot be ruled out from the outset, the DAV demands (i) increased transparency obligations by means of event logging and (ii) increased attention to the AI system when it comes to the requirements and obligations in the context of training data and in connection with transparency obligations.

4.1 AI Systems in the Area of Employment (Annex III.4)

The extensive definition of AI systems in Annex I combined with the definition of high-risk systems in Annex III brings almost all IT-systems used in the area of employment under the scope of the AIA Proposal. In particular, this applies to selection procedures, the assignment of work and the monitoring of employee behaviour. A contradiction exists between the definition of AI systems in Annex I AIA Proposal and the definition of AI in as contained in the European Parliament Resolution of 20th October 2020 on the regulation of civil liability in the use of AI (2020/2014(INL), Art. 3(a)). According to this Resolution, an "AI system" is a software-based system or a system embedded in hardware devices that exhibit intelligence-simulating behaviour by, inter alia, collecting and processing data, analysing and interpreting its environment, and taking action with a certain degree of autonomy to achieve specific goals.

It is imperative that any initiatives which aim at regulating the introduction or use of AI are coordinated with parallel initiatives on liability. The DAV considers that not all software should be defined as AI system, as is currently the case with the AIA Proposal. Such an extensive definition, which affects manufacturers, providers and users equally, violates the entrepreneurial freedom. At the same time, it also affects the preliminary question of subsidiarity, the substantive question of proportionality, the fundamental right to informational self-determination, as well as protection from discrimination.

Furthermore, the AIA Proposal will be difficult to enforce. Enforcement issues are particularly acute for employers who apply AI systems as users. Even when a high-risk AI system would be CE-certified in accordance with the AIA Proposal, an employer can only trust that the AI system indeed fulfils the requirements of the AIA Proposal. The documentation which has to be provided by the supplier may make it easier for the employer to ensure compliance with other provisions, including data protection. However, if an employer adapted an existing, CE-certified high-risk AI system to his own business needs, or turns a non-high-risk AI system into a high-risk AI system by changing the purpose of its use, the employer would become the provider of the AI system with all the associated documentation and information obligations in accordance with Art. 28 AIA Proposal.

When using technical systems in Germany, human rights are not only to be protected through data protection laws, but also through company co-determination. Company co-determination is characterized by comprehensive rights of review and co-determination. This means that small and medium-sized enterprises could quickly become overwhelmed by the additional bureaucratic requirements introduced by the AIA Proposal, hence suffering from considerable competitive disadvantages. At the same time, there is a danger that technical requirements cannot be checked by the users themselves. This lack of effective review by the user is specifically acute in situation when the threshold between users and providers is crossed due to changes to the purpose of an AI system.

The DAV therefore suggests that, at least in the employment context, only those AI systems should be included in the definition of Annex III that include some aspects of machine learning in the sense of Annex I.a of the proposal. This would also bring the

definition closer to the considerations in the European Parliament Resolution of 20 October 2020.

4.2 AI Systems in the Area of Public Administration (Annex III.5)

The legal profession has a particular role to play in upholding the rule of law in the use of AI systems by public administration.

AI systems are used in the allocation of social and economic rights and benefits, in identity verification and in the calculation of eligibility for social benefits. The lack of transparency of AI systems means that discriminatory or otherwise biased results jeopardize rule of law procedures, as they are difficult to detect and challenge before a judge.

Profiling and scoring systems are a particularly critical example due to their significant privacy and data protection risks. All of these can have far-reaching effects on people's access to vital public services and thus on citizens' fundamental rights to social security and social assistance.

The risk of discriminatory profiling or false results goes hand in hand with the risks arising from the processing of sensitive biometric data. Therefore, the DAV demands that the use and application of AI systems that violate access to social rights and benefits must be restricted.

4.3 AI systems in the Area of Law Enforcement (Annex III.6)

In Annex III.6 (a) to (g) AIA Proposal, certain AI systems in the area of law enforcement are defined as high-risk. Any use of AI systems in the area of law enforcement poses a significant risk to the exercise of fundamental procedural rights. Besides the right to an effective remedy and the right to an impartial court, the presumption of innocence and general rights of the defence are particularly affected.

The DAV demands full respect for the principles of transparency and explicability in criminal proceedings. In cases where decisions are based on data or results produced by an AI system, the parties and/or their lawyers must be able to access this AI system to assess its characteristics, the data used and the relevance of the results it provides. Consequently, so-called "strong AI" should only be used to the extent that it is still possible to verify how the machine achieved the proposed result. It must always remain

possible to distinguish the elements resulting from the use of an AI system from the personal considerations of the judge.

This is why the DAV advocates that Art. 13 AIA Proposal must supplemented with a specific reference that AI systems, when used in the judiciary, must not interfere with the right to a fair trial and must not violate the rights of the defence. Considering that the way in which some AI systems produce their results may not be adequately explained (the so-called "black box problem") and the fact that the transparency requirement may not always be met for various reasons, the AIA Proposal needs to provide for other safeguards. For example, a rule could be introduced according to which the result provided by an AI system may not be taken into account in case of doubt or if the transparency or explainability requirements are not met.

Additionally, the DAV demands that transparency obligations should also fully apply in the area of law enforcement. In particular, the exception from transparency obligations in the area of law enforcement according contained in Art. 52 (1) AIA Proposal must be removed. This exception is too far-reaching and jeopardizes the right to a fair trial. Therefore, the DAV supports the EDPB's and EDPS's Joint Opinion of June 2021. This opinion calls for a distinction between AI systems that are used to detect or prevent criminal offences and AI systems that are intended to contribute to the investigation or prosecution of criminal offences. Due to the presumption of innocence, safeguards for prevention and detection must be stronger.[7] Therefore, the DAV is of the opinion that the proposed exception to the principle of transparency should be deleted.

Proposed amendment to Art. 52

(1) 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.~~

[7] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, RN 70.

4.4 AI Systems in the Area of Migration, Asylum and Border Control Management (Annex III.7)

According to Annex III.7 AIA Proposal, certain AI systems in the area of migration, asylum and border control management are classified as high-risk AI systems. The DAV recommends prohibiting the use of AI systems in this area for the reasons already mentioned in section 3.6 above.

4.5 AI Systems in the Justice Area (Annex III.8)

According to Annex III.8 AIA Proposal, certain AI systems in the justice area are classified as high-risk under the heading "administration of justice and democratic processes". The use of AI systems in this area raises many questions, particularly with regards to fundamental rights and the rule of law. Those questions cannot be addressed comprehensively by solely categorizing those AI systems as high-risk. Instead, the DAV recommends that detailed principles and guidelines for the use of AI systems in the justice sector be established. Any AI systems with the purpose of assisting the judiciary should only be introduced if sufficient safeguards against discrimination and bias are in place.

The wording in Annex III.8 AIA Proposal has to be clarified in such a way that a judge must never be allowed to delegate his or her decision-making power in whole or in part to an AI system. Not only automated decision-making by AI systems should be prohibited, but also the use of AI systems that produce "decisions" that could lead a human judge to uncritically adopt them. Such an uncritical use of AI systems would effectively mean that judges are nothing more than “box tickers” for AI systems.

The entire decision-making process must remain human-centred. Judges must take full responsibility for all decisions. The right to a human judge should be guaranteed at all stages of the process. Annex III.8 and Recital 40 should clarify that where an AI system can be used to 'assist' judicial authorities, the possibility is excluded that this AI system actually takes the decisions or formulates the wording of such decisions.

If the use of assistive AI systems in the judiciary leads to automatic adoption of decisions, judges would run the risk of being nothing more than a vehicle for machine-generated decisions. The line between a high-risk classification on the one hand and prohibited AI systems on the other hand should be defined according to whether the

judges concerned are left with sufficient discretion to make an autonomous, impartial and unbiased decision.

Consequently, a judge's decision should be based on reasoning that is sufficiently independent from the prediction of the AI instrument so as to ensure a clear distinction between the two. Each judge should be able to set out his or her own reasoning clearly enough to provide verifiable reasons for following (or rejecting) the decision generated by AI systems. [8] If the final judge-made decision were to degenerate into a mere formality, the right to be heard would be unduly restricted.

The DAV demands that the AIA Proposal should contain concrete provisions targeting specific risks, such as the risk of an unfair procedure. An unfair procedure would exist, among other things, if the parties do not have the opportunity to evaluate, discuss and object to the results of an AI system used in a judicial decision-making process.

In order to ensure respect for fundamental rights and the right to a fair trial, it should be made clear that the AIA Proposal does not preclude the establishment of additional general rules further restricting or prohibiting the use of AI in the areas of justice, including criminal investigations by law enforcement authorities. The use of AI systems in the judiciary must be reconciled with the fundamental values of the legal profession and the guarantee of a fair trial, in particular equality of arms and the impartiality of the court. These fundamental rights must remain guaranteed for all those seeking justice.

5. Requirements for High-Risk AI Systems

Without claiming to be exhaustive, the DAV would like to comment on the following points in detail:

- It is questionable why the AIA Proposal is only applicable to professional users (Art. 3 (4)). Even if this restriction is probably only relevant in a few cases, the question arises as to what this means for non-professional providers and users (such as associations or NGOs). The GDPR, for example, only recognizes an exception for natural persons when conducting exclusively personal or family activities (Art. 2 (2) (c) GDPR). The difference is not convincing.

[8] Enders, Peter, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, 721 (723).

- It is striking that Art. 9 (3) AIA Proposal only requires the risk management measures to take into account the “generally acknowledged state of the art”. This is particularly surprising for high-risk AI systems, since product liability law and German case law require compliance not with the “generally acknowledged” state of the art, but rather the state of the art applicable to science and technology. In view of the strict requirements for high-risk systems on the one hand and corresponding fines and the promotion of innovation on the other hand, a compromise should at least require the latest state-of-the-art technology.
- According to Art. 10 (3) AIA Proposal, “training, validation and test data sets must be relevant, representative, free of errors and complete”. This requirement is designed to be concretized by harmonised standards (Art. 40 AIA Proposal) or implementing acts by the European Commission (Art. 41 AIA Proposal). When industry representatives or the Commission will define these concretizing measures, they should set practicable requirements for the data sets. Art. 10 (3) AIA Proposal should hence be complemented by an additional phrase, e.g. "best possible" or "within reasonable limits". It must also be noted that any data’s relevance, representativeness, completeness or freedom from error can only be assessed against the background of the intended use. This reference to the intended use should be clarified in Art. 10 (3) AIA Proposal by adding "... *shall be relevant (…)* ***with a view to the intended purpose of the high-risk AI system***". Finally, Art. 10 (3) AIA Proposal should be expanded in such a way that this rule can justify the limited processing of personal data, if necessary in a sufficiently anonymised form. Hence, it should be clarified that the interest in obtaining a representative, complete and error-free data set is a legitimate interest within the meaning of Art. 6 (1) (f) GDPR. Nevertheless, in order to achieve a fair balance between the fundamental rights concerned, it is necessary to provide for an exception to this legitimate interest in individual cases. This exception would allow a departure from the quality requirements for training, validation and test data sets; *insofar* the protection of other legal interests (in particular data protection) makes this imperative.
- Art. 28 (1) (b) AIA Proposal requires the user to comply with the provider obligations if the intended purpose of any high-risk AI system is modified, after it has been placed on the market or it has been put into service. It is doubtful that a user will be able to do so without consulting the original provider. In the context

of refinement of IT services, this could lead to the users being fully dependent on the specific knowledge of the original provider. This problem could be circumvented either by granting "access rights" to this knowledge against appropriate remuneration or alternatively by relativizing the obligation contained in Art. 28 (1) (b) AIA Proposal with an “insofar”.

- Art. 28 (2) AIA Proposal partially releases the original provider from liability if an AI system is heavily modified or used contrary to their intended purpose. This is contradictory to both the fundamental approaches of product liability law and the AIA Proposal itself (e.g. Arts. 9 (2) (b), (4) (c); 13 (3) b) (iii) and 14 (2) AIA Proposal). According to these principles, the expected misuse of a system should always be taken into account by the provider and, in the best case (design before instruction), the expected misuse should also be prevented.
- The rules on harmonised standards (Art. 40 AIA Proposal) carry the risk of not being reactive enough in a very innovative field of business (i.e.: the presumption of conformity could prove to be outdated after a short time). The rules on common specifications (Art. 41 AIA Proposal) contain an inherent risk of shifting the power to enact implementing acts in particularly sensitive areas to the Commission (and hence, the administration), particularly in the context of fundamental rights.
- Art. 63 (2) AIA Proposal provides for information to be provided to "relevant national competition authorities". It is unclear whether this provision means that only authorities from individual member states must be informed, or whether the relevant competition authority in each member state must be informed. A clarification would be useful.

6. Protection of Data and Business Secrets

The comprehensive data recording requirements (especially of event logs) and documentation which are required by the AIA Proposal are to be welcomed from the perspective of public security and civil law. However, they collide with the protection of data and business secrets.

The AIA Proposal attempts to reconcile the conflicting protection against threats with data protection in some places (Arts. 10 (5), 29 (6)). It is doubtful that these provisions are sufficient to regulate AI systems, which are often based on big data. This theme needs to be further clarified, particularly also the relationship between the AIA Proposal

and the GDPR. For example, the question arises as to whether event logs may or must be continuously recorded. Under certain circumstances, it could make sense to limit archiving for a certain period of time ("ring storage"). Then data would only be stored for a longer period of time in the event of malfunctioning, accidents or in the case of violations of legal rights. Furthermore, regarding sensitive data as defined in Art. 9 (1) GDPR, an additional authorisation standard should be created, which should go beyond the circumstances currently regulated under paragraph 2. This would be particularly important for AI systems in the medical sector.

Art. 70 AIA Proposal concerns the protection of the confidentiality of information and data by the national authorities and notified bodies specified therein. Here, an extension of the confidentiality obligation to all authorities and bodies, including the Commission, is urgently needed. Insofar as information and data are protected, this protection must also be maintained in the exercise of tasks and activities by all authorities and bodies that come into contact with the information and data.

The same applies to private individuals, insofar as they are also named and addressed as norm addressees in the AIA Proposal. Here, too, comprehensive protection of data and business secrets must be ensured. This concerns on the one hand those providers (cf. the definition in Art. 3 (2)) who themselves develop AI systems or have them developed and place them on the market or put them into operation; and on the other hand the users (cf. the definition in Art. 3 (3)) who use AI systems. In the course of these activities, both providers and users may be involved in the creation, collection and storage of data and trade secrets. In addition, there are far-reaching obligations, such as technical documentation (Art. 11) or record-keeping obligations (Art. 12). Art. 13 also requires the provision of information to users. For high-risk systems, there are information obligations according to Art. 22. Here, too, business secrets may be affected, the protection of which must be ensured. Art. 70 of the AIA Proposal must also include these cases. Irrespective of whether the protection of secrets applies under other legal provisions, it would be insufficient if Art. 70 of the AIA Proposal only addressed individual authorities and bodies.

Insofar as public authorities are affected in their activities, this does not exclude that private individuals also come into contact with business secrets. One example is the inspection of files in the context of exercising information rights. This is another point

that speaks in favour of including private individuals in the scope of the obligations under Art. 70 AIA Proposal.

With regard to the scope of the data and information, there must be no restriction with regard to the protection of secrets. As far as business secrets are concerned, care must be taken to protect these secrets. The Directive on the Protection of Business Secrets contains sufficient exceptions in individual cases (e.g. for the protection of overriding legal interests). Beyond that, there must be no further restrictions or exceptions to the protection of secrets.

For the protection of secrets, there can be no difference between data that is generated and collected by AI systems themselves or between data that is generated and collected by natural persons with the help of AI systems. For this data and information, the protection of secrecy must be upheld without distinction.

The sanctions formulated in Arts. 71 and 72 must correspond to the protection of secrecy. These provisions do not explicitly refer to the protection of confidentiality according to Art. 70. However, the fact that the obligations under Art. 5 and 10 are specifically mentioned brings up the question whether the protection of business secrets should also be covered by this. A clarification would be desirable here, which should explicitly include violations against Art. 70.