DJINGOV
GOUGINSKI
KYUTCHUKOV
VELICHKOV
ATTORNEYS AND COUNSELLORS AT LAW

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

AI ACT: SUMMARY OVERVIEW AND EXPLANATION OF KEY PROVISIONS

This is a summary overview of the new ***Regulation (EU) 2024/1689*** *of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*[1] (the "**AI Act**"). This article also explains the key provisions regarding artificial intelligence ("**AI**") governance in the AI Act.

The AI Act has a direct effect and does not need any implementing legislation in the individual Member States of the European Union ("**EU**").

The AI Act was published in the EU Official Journal on 12th July 2024 and will enter into force on 1st August 2024. It will apply in its entirety from 2 August 2026 with certain exceptions including:

- the prohibition of certain AI practices and the general provisions of the AI Act which start applying from **2 February 2025**;
- the obligations of general-purpose AI model providers and the AI Act provisions on unified AI governance, supervision and sanctions which start applying from **2 August 2025**; and
- the rules regarding the classification of AI systems as high-risk systems based on their intended use (*pursuant to Article 6(1) AI Act*) and the obligations of operators in this respect which start applying from **2 August 2027**; the application of all other rules regarding high-risk AI systems is subject to the general effective date of the AI Act, i.e., start applying from 2 August 2026.

Why do we look at *this EU piece of legislation now, before it has started applying?*

We do it because *the AI Act is likely to affect every business organization, and it is in the best interest of every business organization to know the AI governance rules and align its operations and business development with such rules on time.*

In this article we address and respond to the following questions:

[1] See at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

I. What does the AI Act govern?

1.1. "*Artificial intelligence system*" ("**AI system**") and "*general-purpose AI model*" ("**GPAI model**") are the main concepts pursuant to the AI Act.

1.2. ***AI system*** is defined as a machine-based system that (i) is designed to operate with varying levels of autonomy, (ii) may exhibit adaptiveness after deployment, and (iii) infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

1.3. ***GPAI model*** is a model trained with a large amount of data using self-supervision at scale that displays significant generality and is capable of competently performing a wide range of distinct tasks, regardless of the way the model is placed on the market, and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

1.4. The AI Act governs ***the placing on the market***, ***the putting into service*** and ***the use of AI systems*** in the EU as well as ***the placing on the market of GPAI models***.

1.5. The AI Act does not apply to AI systems, which are used exclusively for military, defense or national security purposes as well as for the purposes of scientific research and development. It does not apply to non-general purpose AI models, either.

II. To which organizations and professionals does the AI Act apply?

2.1. All organizations and professionals that are part of the value and supply chain of an AI system or use an AI system are ***subject to the AI Act***, including those that do or participate in the design and development of such system to those that make the AI system available on the market for commercial and/or organizational purposes of end users (consumers). The AI Act defines all these organizations and professionals collectively as "**operators**".

2.2. ***Operators*** and, respectively, ***obligors*** under the AI Act include (i) the provider and, when applicable, the authorized representative (of the provider), (ii) the product manufacturer, (iii) the importer, (iv) the distributor, and (v) the deployer (the user) of an AI system.

2.3. The AI Act defines operators are follows:

(i) "***provider***" means a natural or legal person, public authority, agency or other body that develops an AI system or a GPAI model or that has an AI system, or a GPAI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

(ii) "***authorized representative***" means a natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a GPAI model to, respectively, perform and carry out on its behalf the obligations and procedures established by the AI Act.

(iii) "***product manufacturer***" as the manufacturer of the product, in which a high-risk AI system is embedded or incorporated, where that product is placed on the market or put into service under the manufacturer's own name or trademark, and the AI Act deems it a provider with regard to obligations and liability.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

(iv) "***importer***" means a natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

(v) "***distributor***" means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market.

(vi) "***deployer***" means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

2.4. The AI Act applies to:

- EU and third-country providers placing an AI system or a GPAI model on the EU market;
- deployers, which have their place of establishment or are located in the EU;
- providers and deployers, which have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union;
- all importers and distributors of AI systems;
- product manufacturers - providers and deployers respectively; and
- authorized representatives of providers, which are not established in the Union.

III. Whose rights and interests are protected?

3.1. The purpose of the AI Act is to ensure the protection of natural persons in respect of whom AI systems or GPAI models are used and, as a result, the fundamental rights and interests of these persons – such as life, health, privacy, liberty, confidentiality of personal data and personal communications – are at risk of being infringed. The AI Act refers to these subjects as "***affected persons***".

3.2. The ***affected persons*** enjoy the protection of the AI Act provided that they are in the EU.

3.3. Affected persons are entitled to lodge a complaint to the relevant market surveillance authority if they consider that there has been an infringement of the AI Act.

3.4. Any affected person subject to a decision, taken by the deployer on the basis of the output from a high-risk AI system, who considers that the decision results in an adverse impact on his/her health, safety, or fundamental rights, has the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

IV. What is the regulatory approach?

4.1 According to the AI Act, the AI shall be "*governed*", and the AI governance shall be approached in a risk-based manner. The "*risk*" is defined as a combination of the likelihood for a relevant harm to occur and the severity of that harm. AI systems (and GPAI models, respectively) are categorized in accordance with the risk of harm to the health, safety and/or fundamental human rights arising from the use of these systems and models. The AI technology *per se* is not deemed harmful.

4.2. There are four different levels of risk, and, respectively, four sets of requirements for AI systems.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

Level of Risk	Requirements and restrictions	Bound operators
Unacceptable	• ***Comprehensive list*** of prohibited practices	All operators.
High	• Classification of high-risk AI systems in accordance with ***established criteria and a list***; • ***Legal compliance*** requirements; • Independent conformity assessment and certification; • *CE* marking to indicate conformity; • EU database registration; • ***Obligations*** for the operators; • Defining the ***allocation of responsibility*** between operators across the high-risk AI systems value chain.	All operators.
Limited	• Applies to AI systems designed to interact directly with natural persons and to AI systems that generate synthetic audio content, images, video or text; • ***Obligations*** for transparency, disclosure and protection of the rights and freedoms of natural persons.	Providers (or authorized representatives) and deployers.
Minimal or unidentified risk	There are no requirements or restrictions.	Not applicable.

4.3. ***Both providers and deployers of all AI systems*** have the obligation to ensure that their employees, contractors, and vendors involved in the operation and/or use of AI systems have the necessary competence and adequate level of awareness and sensitivity (i.e., through training) in the area of AI and AI governance.

V. Which AI practices are prohibited?

It is prohibited to place on the market, put into service, and use AI systems that can or are intended to:

5.1. manipulate natural persons, including by impairing their ability to make an informed decision or by exploiting their vulnerability due to their age, disability or a specific social or economic situation, and in this way causes or is reasonably likely to cause significant harm to such persons;

5.2. profile natural persons which leads or may lead to detrimental or unfavorable treatment of these persons;

5.3. execute risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence;

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

5.4. create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

5.5. infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

5.6. execute categorization of natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation (exception: lawfully acquired biometric datasets for law enforcement purposes); and

5.7. be used for 'real-time' remote biometric identification in publicly accessible spaces for the purposes of law enforcement (certain strict and exhaustive exceptions are envisioned: for the purposes of preventing abduction, trafficking in human beings, terrorism, as well as certain other criminal offences).

VI. Which AI systems are defined as high-risk?

6.1. AI systems are classified as high-risk when the following conditions are fulfilled:

(i) the AI system is intended to be used as a safety component of a product, or the AI system itself is a product regulated by the EU harmonization legislation; and

(ii) the product whose safety component pursuant to item (i) hereinabove is the AI system, or the AI system, itself as a product, is required to undergo a third-party conformity assessment pursuant to the EU harmonization legislation.

6.2. For example, as high-risk would be classified such AI systems which are a safety component of, or themselves provide safety for, machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, in vitro diagnostic medical devices, automotive, and aviation.

6.3. High-risk AI systems are the AI systems listed in any of the following eight areas (*Annex III of the AI Act*):

- ❖ biometrics in so far as their use is permitted under relevant EU or national law;
- ❖ critical infrastructure;
- ❖ education and vocational training;
- ❖ employment, workers management and access to self-employment;
- ❖ access to and enjoyment of essential private services and essential public services and benefits;
- ❖ law enforcement, in so far as the use of the AI systems is permitted under relevant Union or national law;
- ❖ migration, asylum and border control management, in so far as their use is permitted under relevant EU or national law; and
- ❖ administration of justice and democratic processes.

The AI Act provides for specific exceptions under certain conditions. If an AI system in any of the eight areas does profiling of natural persons, it will be unconditionally classified as high-risk.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

VII. What are the principal requirements to high-risk AI systems?

High-risk AI systems must meet the following requirements:

7.1. Continuous compliance of the AI system with the relevant requirements set out in the AI Act;

7.2. A risk management system - set up, implemented, documented and maintained;

7.3. Data governance and management of training, validation and testing data sets used for the design and development of the AI system;

7.4. Preparing and keeping technical documentation;

7.5. Keeping records (registers) of automatic event logs;

7.6. Transparency (as of the design stage) and information disclosure;

7.7. Human oversight (embedded into the AI system at the design and development stage);

7.8. Accuracy, (cyber)security and reliability (embedded in the AI system at the design and development stage).

VIII. What are the main obligations of high-risk AI system operators? How is responsibility allocated among operators?

8.1. ***Providers*** of high-risk AI systems shall:

- ensure that their high-risk AI systems are compliant with the requirements set out in the AI Act;
- indicate their name, registered company name or registered trademark, the contact address;
- have a quality management system in place;
- keep technical documentation about the AI system;
- keep the logs automatically generated by their high-risk AI systems;
- ensure that the high-risk AI system undergoes the relevant conformity assessment procedure prior to its being placed on the market or put into service;
- draw up and submit an EU declaration of conformity (including conformity with the GDPR) and affix the *CE* marking to the high-risk AI system;
- register the AI system in the EU database;
- establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system;
- in case of nonconformity, immediately take the necessary corrective actions to bring the AI system into conformity, withdraw it, disable or recall it, as appropriate, and inform the competent market surveillance authority;
- cooperate with competent national authorities and upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in the AI Act;
- ensure that the high-risk AI system complies with accessibility requirements in accordance with applicable law;
- notify the national market surveillance authority of any serious incident after the AI system has been placed on the market.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

8.2. ***Importers*** of high-risk AI systems shall:

- ensure that the relevant high-risk AI system provider has fulfilled the compliance requirements before they place on the market or put into service the AI system concerned;
- do not place a high-risk AI system on the market or into service until it has been brought into conformity, where they have sufficient reason to consider that the AI system is not in conformity with the AI Act. In certain high-risk circumstances, they shall also inform the provider of the system and the market surveillance authority to that effect;
- cooperate with the relevant competent authorities in any action those authorities take in relation to a high-risk AI system placed on the market by the importers, and provide these authorities, upon a reasoned request, with all the necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in the AI Act;
- ensure that storage or transport conditions do not jeopardize its compliance with the requirements set out in the AI Act;
- keep a copy of the conformity certificate, the instructions for use, and the EU declaration of conformity for a period of 10 years after the high-risk AI system has been placed on the market or put into service.

8.3. ***Distributors*** of high-risk AI systems shall:

- verify that the high-risk AI system bears the required CE marking, accompanied by a copy of the EU declaration of conformity and instructions for use, and ensure that the AI system provider and importer have complied with their respective obligations laid down in the AI Act, before making a high-risk AI system or the product in which the AI system is incorporated available on the market;
- do not make the high-risk AI system available on the market until the system has been brought into conformity when they consider or have a reason to consider that a high-risk AI system is not in conformity with the requirements set out in the AI Act. In certain high-risk circumstances, they shall also inform the provider of the system, the importer and the market surveillance authority to that effect;
- cooperate with the relevant competent authorities in any action those authorities take in relation to a high-risk AI system made available on the market by the distributors, and provide these authorities, upon a reasoned request, with all the necessary information and documentation to demonstrate the conformity of the distributed high-risk AI system with the requirements set out in the AI Act;
- ensure that storage or transport conditions do not jeopardize its compliance with the requirements set out in the AI Act;
- keep a copy of the conformity certificate, the instructions for use, and the EU declaration of conformity for a period of 10 years after the high-risk AI system has been placed on the market or put into service.

8.4. ***Deployers*** of high-risk AI systems shall:

- take appropriate technical and organizational measures to ensure they use such AI systems in accordance with the instructions for use accompanying these systems;
- assign human oversight in relation to the AI system to natural persons who have the necessary competence, training and authority, and support;

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

- to the extent they exercise control over the input data, deployers shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system;
- monitor the operation of the high-risk AI system on the basis of the instructions for use and inform providers immediately in case of identified discrepancies or non-conformities;
- where they have identified a serious incident or risk, they shall immediately inform, first, the provider, and then the importer or distributor, and the relevant market surveillance authorities;
- keep the logs automatically generated by the high-risk AI system, to the extent such logs are under their control, for an appropriate period, but in any case, for at least six months unless provided otherwise under applicable law on personal data protection;
- inform the natural persons that they are subject to the use of the high-risk AI system if that system is used for or assists in the decision-making in relation to such natural persons;
- inform the affected workers that they will be subject to the use of the high-risk AI system before the deployers, as employers, put into service or use such high-risk AI system at the workplace;
- carry out fundamental rights impact assessment[2]; further to the assessment, notify the competent market surveillance authority of the results thereof.

8.5. ***Allocation of responsibility among operators*** across the high-risk AI system value chain

(i) Any distributor, importer, deployer or other third-party will be considered to be a provider of a high-risk AI system when it:

- puts its name or trademark on a high-risk AI system already placed on the market or put into service;
- makes a substantial modification to a high-risk AI system, which has already been placed on the market or has already been put into service, in a way that it remains a high-risk AI system in accordance with the AI Act; or
- modifies the intended purpose of an AI system in a way that the AI system becomes a high-risk AI system in accordance with the AI Act.

In these cases, the provider who has originally placed the AI system on the market or into service, no longer holds the capacity of and does not bear responsibility as a provider.

(ii) In respect of high-risk AI systems that are a safety component of a product which falls within the scope of the EU harmonization legislation based on the *New Legislative Framework*, the product manufacturer should comply with the obligations of the AI high-risk provider when:

- the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer; or
- the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

[2] The assessment shall be made against the minimum criteria set out in the AI Act and may be combined and build on the impact assessment of the AI system in respect of data protection (pursuant to art. 35 GDPR).

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

IX. How shall a conformity assessment of high-risk systems be done?

9.1. In respect of high-risk AI systems, which fall within the scope of EU internal market legislation for products and services, the conformity assessment procedures under the relevant legislative act are to be applied.

9.2. All AI systems in high-risk areas except biometric identification and categorization are subject to an internal control review.

9.3. AI systems in the field of biometric identification and categorization, where standard or common specifications have been applied, shall undergo an internal control review or conformity assessment procedure based on a quality management system assessment involving a notified body. If no standard or common specifications are applied (or are not available), AI systems in the field of biometric identification and categorization shall be assessed for conformity on the basis of a quality management system assessment involving a notified body.

X. What obligations do operators have in respect of AI systems intended to interact directly with natural persons and AI systems that generate synthetic content?

10.1. ***Providers*** shall:

- ensure that the AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person (this obligation does not apply to AI systems authorised by law to detect/investigate criminal offences, unless those systems are available for the public to report a criminal offence);
- ensure that the output of the AI systems, including general-purpose AI systems, are marked in a machine-readable format and detectable as artificially generated or manipulated. The labelling of artificially generated/processed content shall be carried out according to codes of practice.

10.2. ***Deployers*** shall:

- inform the natural persons, which are exposed to an emotion recognition system or a biometric categorisation system, and process the personal data in accordance with applicable data protection law (this obligation does not apply to AI systems used for detection/investigation of criminal offences);
- disclose that the generated image, audio/video content constituting a deep fake, has been artificially generated or manipulated (this obligation does not apply to AI systems used for detection/investigation of criminal offenses);
- deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated;
- the information shall conform to the applicable accessibility requirements and is without prejudice to other transparency obligations laid down in Union or national law;
- detection/ labelling of artificially generated/processed content shall be conducted according to codes of practice.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

XI. How are GPAI models classified?

11.1. GPAI models are subject to a separate classification. The AI Act sets forth the applicable obligations for the operators based on the risks that the respective GPAI model may pose. The Regulation differentiates among the following:

(i) systemic-risk GPAI models;

(ii) "standard" GPAI models; and

(iii) GPAI models that are released with a free and open-source license that allows for access, usage, modification, and distribution of the model, and whose parameters are made publicly available ("**GPAI models with a free and open-source license**").

11.2. A GPAI model is of systemic risk when it satisfies one of the following conditions: (1) the GPAI model has high impact capabilities assessed by appropriate technical methodologies (a GPAI model is presumed to have high impact capabilities when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}), or (2) the GPAI model is considered, within a decision of the European Commission, acting upon its own initiative or following a priority signal of the expert group, to have a capability or impact equivalent to that assessed by appropriate technical methodologies, taking into account the criteria in *Annex XIII of the AI Act*.

11.3. The most comprehensive group of obligations is assigned to the operators of systemic risk GPAI models, whereas GPAI models with a free and open-source license with no systemic risk are excluded from some of the general obligations applicable to the operators of GPAI models.

XII. What obligations do providers of GPAI models have?

12.1. All ***GPAI model providers*** shall:

- produce and update the technical documentation of the GPAI model, which shall be made available to the authorities upon request (not applicable to models with a free and open-source license with no systemic risk);
- prepare, update and provide information and documentation to AI system providers that intend to integrate the GPAI model into their AI systems (not applicable to models with a free and open-source license with no system risk);
- implement a copyright compliance policy;
- make publicly available a summary of the content used to train the GPAI model, on the basis of a template.

12.2. In addition to the above, ***providers*** of GPAI models that raise a systemic risk are required to:

- notify the European Commission within two weeks of establishing that the requirements for designation of the model as a GPAI model posing systemic risk have been met;
- assess the GPAI model in accordance with standardized protocols and tools;
- assess and mitigate possible systemic risks;
- document and report serious incidents and possible corrective actions;
- ensure an appropriate level of cybersecurity;

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

- comply with the obligations by implementing codes of practice pending publication of a harmonized standard; for providers that comply with a European harmonized standard, there is a presumption of compliance as long as the standards cover the specified obligations.

12.3. ***Representatives*** of GPAI model providers, except of GPAI models with a free and open-source license with no systemic risk, are obliged to:

- verify that the Provider has prepared the technical documentation in accordance with the AI Act;
- keep a copy of the technical documentation at the disposal of the competent authorities;
- provide to the AI Office the information and documentation necessary to demonstrate compliance with the obligations hereunder;
- represent the Provider before the authorities and persons concerned in relation to matters under the AI Act.

XIII. How are AI unified governance and supervision provided? What are the sanctions?

13.1. Competent authorities for unified AI governance

(i) At the EU level, competent authorities will include:

- ***European Artificial Intelligence Office*** (the "**AI Office**"), supported by a scientific panel of independent experts;
- ***European Artificial Intelligence Board*** (with status and functions like the European Data Protection Board in the area of data protection), supported by an advisory forum which provides technical expertise and advice;

(ii) At the EU Member State level, competent authorities include:

- at least one ***notifying authority*** (responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring);
- ***notified bodies***, which carry out conformity assessments of high-risk AI systems;
- ***market surveillance authorities***, which will ensure the implementation and enforcement of the AI Act;
- the activities of the market surveillance authorities will neither limit nor preempt the powers that other national competent authorities may have over operators under other applicable law - for example, in Bulgaria, such authority is the Commission for Personal Data Protection with regard to compliance with personal data protection requirements.

13.2. Supervision bodies with sanctioning competences:

(i) the European Commission (directly or through the AI Office);

(ii) a National Market Surveillance Authorities in each Member State; and

(iii) the European Data Protection Supervisor (in certain cases in respect of EU institutions, agencies and bodies regulated by the AI Act).

13.3. ***Liability. Sanctions***.

(i) The AI Act sets forth material sanctions for non-compliance. These may reach up to EUR 35 million or 7 % of the total worldwide annual turnover for the preceding financial year, or up to

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

EUR 7.5 million or 1% of the total worldwide annual turnover for the preceding financial year, whichever sum is higher (and for SMEs – whichever sum is lower).

(ii) The AI Act delegates to the EU Member States the power to set out in their national law specific administrative sanctions up to the maximum amounts provided for in the AI Act, and to ensure that these sanctions are accurately and effectively applied. The administrative sanctions must be effective, proportionate and dissuasive, and shall respect the legitimate interests of small and start-up providers.

(iii) Procedural rules shall also be set forth in the national legislation.

XIV. Any recommended first steps?

We would suggest the following steps as a good start in ensuring compliance with the AI Act:

- Conduct an audit to identify what AI systems are or could be used specifically in your business. If you are developing or supplying AI systems or GPAI models, carry out an analysis to establish which AI Act category they fall into.
- Cease the use of prohibited AI practices before the AI Act prohibition on these starts to apply.
- Adopt and start implementing an AI policy or internal rules to ensure that AI systems are implemented and used in accordance with the key provisions of the AI Act;
- Conduct appropriate staff training on AI and AI governance further to the AI Act.

* * *