Overview of the AI Act

What is the aim of this briefing?

This briefing does not contain legal advice: our aim is to provide an overview of the provisions in the hope of sparking interest, making the topic accessible to people of different disciplines and thereby furthering debate. If you have found this overview useful, but have identified areas of concern, we would love to hear from you and engage with your thoughts.

What does the AI Act regulate?

The AI Act regulates specific types of AI systems: prohibited AI systems (Art. 5), high-risk AI systems (Art. 6) and AI systems with limited risk (Art. 52).

Prohibited AI systems cannot enter the market or be put into service in the European Union.

High-risk AI systems can be put on the market or into service in the European Union if the system meets a number of requirements. The AI Act defines several roles which are obliged to ensure that these requirements are met: the provider, the importer, the distributor and the user.

Limited risk AI systems do not have to meet the requirements for high-risk AI systems. Instead, these systems must provide a certain level of transparency about the system in its outputs.

What is not regulated by the AI Act?

The AI Act does not regulate low-risk AI systems as well as AI systems developed purely for research purposes.

AI systems developed or used exclusively for military purposes are exempt from the scope of this Regulation (Art. 2 para. (3)). Similarly, public authorities in a third country and international organisations using AI systems in the framework of law enforcement and judicial cooperation agreements with the European Union or with one or more Member States are also exempt from compliance (Art. 2 para. (4)).

The AI Act does not contain any provisions regarding liability. It also does not contain provisions related to labour, to the environment or competition. It does not regulate widely-used search or recommendation algorithms – these are in some limited aspects and under specific conditions regulated by the Digital Markets Act and the Digital Services Act, respectively.

Art. 83 also contains a "grandfathering clause" which exempts those AI systems from compliance with the regulation which have been placed on the market or put into service before the AI Act comes into force, unless a significant change in their design or intended purpose takes place.

What types of systems does the AI Act define as "artificial intelligence"?

The AI Act defines AI systems as software developed using specific techniques and approaches which can generate outputs according to human-defined objectives (Art. 3 point (1)).

The technologies considered relevant are machine learning approaches, logic- and knowledge-based approaches and statistical approaches (Annex I).

Machine learning approaches include supervised, unsupervised and reinforcement learning. The methods used are not explicitly specified, with the exception of deep learning.

Logic- and knowledge-based approaches include:

- knowledge representation,
- inductive (logic) programming,
- knowledge bases,
- inference and deductive engines,
- (symbolic) reasoning,
- expert systems.

Statistical approaches include Bayesian estimation, search and optimisation methods.

This list of techniques and approaches may be amended at a later point in time to reflect the development of new technologies that are similar to those already included (Art. 4).

Which AI systems are prohibited?

The AI Act identifies four practices which shall be prohibited in the European Union (Art. 5). Two of these prohibitions apply to systems deployed by any actor, namely: AI systems that use **subliminal techniques** and systems **exploiting vulnerabilities based on age, physical or mental disability**. The other two apply to systems deployed by public authorities, namely: AI systems used for **social scoring** and **real-time remote biometric identification systems**.

AI systems deploying subliminal techniques (Art. 5 para. (1a))

The AI Act prohibits: "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 harm."

This provision aims to prohibit the manipulation of people if this leads to physical or psychological harm. AI systems should therefore not be developed in a way that users might be tricked into actions which go against their interests. Due to the lack of a definition of these "subliminal techniques beyond a person's consciousness," this provision is unfortunately relatively vague. One criticism which has already been brought forth by Access Now regards the exclusion of economic harm from this prohibition.

AI systems exploiting vulnerabilities (Art. 5 para. (1b))

The second prohibited type of system is defined as follows: "the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm."

The intention of this provision is to prevent algorithmic discrimination based on a person's capacities if this discrimination leads to physical or psychological harm. As mentioned further above, economic harm is excluded from this prohibition.

Social scoring (Art. 5 para. (1c))

This prohibition concerns: "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."

As mentioned before, this prohibition applies only to AI systems used by public authorities (or on their behalf). It aims to prevent discrimination of public authorities against individuals or groups based on their history (i) or their actions (ii) – or both. This does not include so-called predictive policing, as this use of AI systems is included in Annex III para. (6c) as high-risk, although the vague definition of social scoring leaves enough room to interpret certain kinds of predictive policing as social scoring.

'Real-time' remote biometric identification systems (Art. 5 para. (1d))

The final prohibition concerns: "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, 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/JHA62 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."

The prohibition of 'real-time' remote biometric identification systems has so far been the most hotly contested by different stakeholders, most prominently the European Data Protection Supervisor. Several key issues with this provision are the scope of the prohibition, which applies only to 'real-

time' and 'remote' uses of biometric identification systems, namely in 'publicly accessible spaces' (which are defined as physical spaces). The prohibition does not extend to private individuals or companies seeking to use this type of technology.

What is considered a high-risk AI system?

In the AI Act, high-risk AI systems feature prominently due to the aim of the Regulation: to reduce as much as possible the risk of harm for uses of AI that can have a large negative impact and where the likelihood of problems occurring is particularly high.

High-risk AI systems fall into one of two categories: either they are or form part of a **product which is subject to product safety legislation** (Art. 6 para. (1)), or the **use case is listed as high-risk** (Art. 6 para. (2)).

AI systems subject to product safety legislation

AI systems are to be considered high-risk if they are products (or safety components of products) which are covered by harmonised legislation (Art. 6 para. (1a) and subject to third-party conformity assessments (Art. 6 para. (1b)). It is important to stress that only those systems that fulfil the criteria of both Art. 6 para. (1a) and Art. 6 para. (1b) are considered high-risk: if only one of these criteria is met, the system will not be considered high-risk.

The list of Union harmonisation legislation is provided in Annex II and is exhaustive, because there is no provision allowing for an update of this Annex. Annex II itself is divided into two sections: harmonisation legislation based on the New Legislative Framework (Section A)[1] and other Union harmonisation legislation (Section B).[2]

High-risk use cases

Beyond those use cases for AI in sensitive areas already covered by existing legislation, the AI Act defines a list of eight use case "areas" which are considered high-risk (Art. 6 para. (2)) in Annex III. The general areas of use are exhaustive, but the European Commission may adopt delegated acts to add systems that fall into a specified area and pose a risk to health, safety or fundamental rights which is equal to or greater than that of the applications already listed (Art. 7). Again, both of these criteria must apply if an application is to be added.

The first use case area is the **biometric identification and categorisation of natural persons**. In this area, the use of AI for 'real-time' and 'post' remote biometric identification of natural persons is listed as an application.

Next, the **management and operation of critical infrastructure** is listed as a high-risk area. The corresponding application is the use of AI systems as safety components in the management and

[1] Annex II, Section A: Directive EC 2006/42/EC, Directive 2009/48/EC, Directive 2013/53/EU, Directive 2014/33/EU, Directive 2014/34/EU, Directive 2014/53/EU, Directive 2014/68/EU, Regulation (EU) 2016/424, Regulation (EU) 2016/425, Regulation (EU) 2016/426. Regulation (EU) 2017/745, Regulation (EU) 2017/746

[2] Annex II, Section B: Regulation (EU) No 300/2008, Regulation (EU) No 168/2013, Regulation (EU) No 167/2013, Directive 2014/90/EU, Directive (EU) 2016/797, Regulation (EU) 2018/858, Regulation (EU) 2018/1139

operation of road traffic and the supply of water, gas, heating and electricity. Notably, telecommunications infrastructure is excluded from consideration as critical infrastructure.

The third area concerns **education and vocational training**. Two applications are listed here, namely:

a) AI systems used for determining access or assigning natural persons to educational/vocational training institutions and
b) AI systems for assessing students in these institutions and for assessing participants in tests required for admission to these institutions.

Surprisingly, the monitoring of students is not listed as a high-risk application.

As fourth area, the field of **employment, workers management and access to self-employment** is listed. The two applications which are included here refer to:

a) AI systems used in recruitment or for the selection of persons in the context of employment and
b) AI systems used to make decisions on promotion or termination of employment contracts, task allocation or monitoring and evaluating the performance or behaviour of workers.

The fifth area concerns the **access to and enjoyment of essential private services and public services and benefits**. Three applications are defined in this area:

a) AI systems used by or on behalf of public authorities to evaluate eligibility for or manage access to public assistance benefits and services;
b) AI systems used to evaluate the creditworthiness or establish the credit score of natural persons (except for those used by small-scale providers for their own use); and
c) AI systems used in the context of dispatching emergency services.

It is noteworthy that applications related to insurance are currently exempted from this field.

In the sixth area of high-risk use cases – namely in **law enforcement** –, a total of seven applications are listed:

a) AI systems used by law enforcement authorities for assessing the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
b) AI systems used by law enforcement authorities as polygraphs or to detect the emotional state of natural persons;
c) AI systems used by law enforcement authorities to detect deep fakes;
d) AI systems used by law enforcement authorities to evaluate the reliability of evidence;
e) AI systems used by law enforcement authorities to predict the occurrence or reoccurrence of criminal offences based on profiling of natural persons or to assess the personality traits and characteristics or past criminal behaviour of natural persons or groups;
f) AI systems used by law enforcement authorities for profiling natural persons in the course of detection, investigation or prosecution of criminal offences;
g) AI systems to be used for crime analytics regarding natural persons, allowing law enforcement authorities to process large data sets to identify unknown patterns or discover hidden relationships in the data.

Importantly, six of these applications only concern systems used by law enforcement authorities. This means that applications used by other organisations on behalf of law enforcement authorities

to e.g. detect deep fakes are not currently categorised as high-risk. Location-based predictive policing, also known as hot spot policing, is not included in the definition of e) - despite having a discriminatory impact, this type of predictive policing would not be regulated as a high-risk AI system. Similarly, AI systems used for crime analytics described in point g) do not include systems used to process large data sets about groups of persons.

The seventh use case area comprises applications related to **migration, asylum and border control management**. Four applications are defined in this field:

a) AI systems used by authorities with responsibilities in these areas as polygraphs or to detect the emotional state of a natural person;
b) AI systems used by these authorities to assess a risk (including security risks, risk of irregular migration and health risks) posed by natural persons entering or having entered a Member State;
c) AI systems used by these authorities to verify the authenticity of travel documents and to detect non-authentic documents by checking security features; and
d) AI systems used to assist these authorities in examining applications for asylum, visa and residence permits and assess complaints related to the eligibility of natural persons applying for a status.

Points c) and d) lack clarity in their formulation in the original text, as the sentences are not well structured.

The eighth and final area of use cases concerns the **administration of justice and democratic processes**. Only one application is listed here, namely AI systems used to assist a judicial authority in researching and interpreting facts and the law (and applying the law to a concrete set of facts).

My AI system is considered high-risk. What do I need to do?

Firstly, you need to ensure that your high-risk AI system complies with the requirements for high-risk AI systems (Art. 8): the AI system must have an appropriate **risk management system** in place (Art. 9), the **data set quality** must be ensured and appropriate **data governance** measures must be implemented (Art. 10). The **technical documentation** must be complete (Art. 11) and a system for **recording logs** in place (Art. 12). The system itself must be designed in a way that **humans can understand** what is happening and it must be accompanied by **instructions for use** (Art. 13). These measures are key to ensuring another requirement, namely **human oversight** (Art. 14). Finally, the AI systems must meet certain levels of **accuracy, robustness and cybersecurity** (Art. 15).

Next, you need to understand your **role** with regards to the high-risk AI system: are you a provider, an importer, a distributor or a user? The AI Act lays down obligations for each of these roles, which will be explained in more detail further below.

Obligations of providers of high-risk AI systems

Art. 3 para. (2) defines providers as "any natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting into service under its own name or trademark, whether for payment or free of charge". This definition on the one hand excludes researchers, unless the AI application is made available to others under the name or trademark of the research group. On the other hand, the definition of 'provider' includes AI systems made available free of charge as open-source models.

Providers of high-risk AI systems face the most extensive set of obligations. Art. 16 sets out most of the obligations of providers, which are then elaborated in more detail in the following provisions.

Conformity with requirements for high-risk AI systems (Art. 16)

Every provider must ensure that their high-risk AI system fulfils the requirements for high-risk AI systems (see above). As set out in Art. 40 and 41 respectively, the simplest way to ensure conformity is to adopt **standards** (which will be developed by standardisation organisations) or adhere to **common specifications** (which will be developed by the European Commission if no adequate standards are available). If an AI system is **developed for a specific context**, it will be considered compliant with Art. 10 para. (4), which obliges provider to take into account specific geographical, behavioural or functional settings of the context in which the system will be used (Art. 42 para. (1)). Using **standards for cybersecurity** will also ensure compliance with Art. 15, setting out cybersecurity obligations for high-risk AI systems (Art. 42 para. (2)).

Technical documentation (Art. 18 + Annex IV)

One of the more complex requirements for high-risk AI systems is the technical documentation called for in Art. 11 and described in Annex IV. Providers must draw up the technical documentation (Art. 18) and make it available to importers or distributors, as this is also a cornerstone of their obligations. The technical documentation must be retained for 10 years in accordance with Art. 50. It is important to note that the technical documentation will not reach the user: the provider must make it available to the conformity assessment body and, if applicable, the importer.

The technical documentation consists of eight broad categories: a **description of the AI system**, a description of its **elements and development process**, information about **monitoring and functioning of the system**, a description of the **risk management system**, a description of c**hanges made during the AI system's lifecycle**, a list of **harmonised standards** applied (or other solutions to the requirements for high-risk AI systems), a copy of the **EU declaration of conformity**, and – last but not least – a description of the **post-market monitoring system**.

Of these categories of documents, three are very detailed and merit a closer look.

The **general description of the AI system** should include information about the AI system's **intended purpose**, about its **developers** and about the **date and version** of the system. The v**ersions of software or firmware** and any update requirements also need to be specified. This document shall further include the description of **all forms of the AI system** available on the market and of the **required hardware** for the AI system. The general description must also include **instructions of use** for the user and (where applicable) installation instructions. In addition, and if applicable, the provider needs to explain how the AI system **interacts with hardware or software** which is not part of the system. If the AI system is a component of a product, **photographs or illustrations** must be submitted to show external features, marking and internal layout of the product.

With the **description of elements of the AI system and processes for its development**, details need to be provided on the technical design and sources of the AI system. This includes details on the **methods and steps performed during development**, including the use of pre-trained systems or tools and how these have been used, integrated or modified. Secondly, the **design specifications** need to be made transparent: the logic of the AI system and the algorithm, the key design choices (including rationale and assumptions made), the main classification choices, the parameters chosen

for optimisation and their weight, and which trade-offs were made to comply with the requirements for high-risk AI systems. Furthermore, the **system architecture** has to be explained, including how components relate to each other and which computational resources used to train, test and validate the system. The **validation and testing procedures** shall also be detailed: which validation and testing data and which metrics were used to measure accuracy, robustness, cybersecurity and other requirements (as well as potentially discriminating impacts, although this is not defined more precisely), and a copy of the test logs and dated and signed test reports (also regarding pre-determined changes). Likewise, this description must include an assessment of the required **human oversight measures** and any technical measures to facilitate the interpretation of the AI system's outputs. Where relevant, the **data requirements** also need to be included as datasheets describing the training methodologies, techniques and data sets used – along with the provenance of these data sets, their scope and main characteristics, and how the data sets were obtained, selected, labelled and cleaned. Where applicable, any **pre-determined changes** to the AI system and its performance have to be specified, as well as the technical solutions to ensure continuous compliance despite these changes.

The documents containing information about the **monitoring, functioning and control of the AI system** need to include information about its **capabilities and limitations in performance** (including the degrees of accuracy for specific persons or groups of persons) and the overall expected level of accuracy when the AI system is used for its intended purpose. Also, the foreseeable **unintended outcomes and sources of risk to health and safety, fundamental rights and discrimination** when using the AI system for its intended purpose must be detailed. In addition, the necessary **human oversight measures** must be described, including the technical solutions to facilitate the interpretation of outputs. Finally, the provider must include any specifications regarding the input data in this set of documents.

Quality management system (Art. 17)

Providers of high-risk AI systems shall implement and document a quality management system, which must be retained for at least 10 years (Art. 50). This shall cover at least:

- A **strategy for regulatory compliance**, including conformity assessment procedures and procedures for managing modifications of the AI system;
- Techniques, procedures and systematic actions to be used for the **design**, **design control** and **verification**;
- Techniques, procedures and systematic actions to be used for the **development**, **quality control** and **quality assurance**;
- Procedures for the **evaluation**, **testing** and **validation** of the AI system for **before**, **during** and **after the development** of the system, including the **frequency of these procedures**;
- **Technical specifications and standards** to be applied to the system and, if the relevant harmonised standards are not applied in full, the means to ensure compliance with the requirements for high-risk AI systems;
- Systems and procedures for **data management** performed before and in order to place the system on the market, including:
    - data collection,
    - data analysis,
    - data labelling,

    - data storage,
    - data filtration,
    - data mining,
    - data aggregation, and
    - data retention;
- A **risk management system** as described in Art. 9, which shall be continuous throughout the lifecycle of the system and include regular and systematic updates. This risk management system shall: identify and analyse risks; estimate and evaluate the risks associated with the use of the system in accordance with its intended purpose as well as reasonably foreseeable misuse; other risks identified during post-market monitoring; and the adoption of risk management measures. Through the risk management system, the residual risk shall be minimised to an acceptable level – and the residual risk must be made clear to users. Appropriate risk management measures must **eliminate or reduce risks** through the design and development of the high-risk AI system; **mitigate or control risks** that cannot be eliminated; and provide **sufficient information** (Art. 13) and **training** to the user. The risk management system must take into account the technical knowledge, experience, education and training of the user as well as the environment in which the high-risk AI system is intended to be used. All risk management measures should be identified through testing, which should be suitable to achieve the intended purpose and can be performed at any time prior to placing the system on the market, using preliminary metrics and probabilistic thresholds which are appropriate for the intended use.
- A **post-market monitoring system** as described in Art. 61, which is proportionate to the nature of the AI technology used and the risks of the AI system and based on a d**ocumented monitoring plan** (which is part of the technical documentation). Post-market monitoring should actively and systematically collect, document, and analyse relevant data on performance of high-risk AI systems throughout its lifetime, allowing the provider to **evaluate continuous compliance** with the requirements for high-risk AI systems. The European Commission will adopt a template for post-market monitoring plans and provide a list of elements to be included in this plan. For those high-risk AI systems which are themselves products or part of products requiring conformity assessments (Annex II), the requirements for post-market monitoring of the AI system shall be included in the existing post-market monitoring of the applicable product safety legislation.
- Procedures for **reporting serious incidents or malfunctions** to the market surveillance authority in accordance with Art. 62. Serious incidents or malfunctions must be reported immediately and no later than 15 days after the provider becomes aware of the problem. The European Commission will develop guidance for reporting issues within 12 months of this Regulation entering into force.
- Procedures for **communicating with national authorities**;
- Systems and procedures for **keeping records (logs)** as required by Art. 20. If these logs are accessible to the provider, they must be kept for as long as appropriate.
- A **resource management** system which includes measures related to the security of the supply;
- An **accountability framework** for management and office staff.

Conformity assessment procedure (Art. 19 + 43)

Before placing a high-risk AI system on the European market, the provider has to undergo a conformity assessment (Art. 19). Every time the high-risk AI system is modified substantially, a new conformity assessment is necessary. Self-learning AI systems only need to undergo new conformity assessments if the substantial modification is not predetermined by the provider and included in the technical specifications. There are three options for conformity assessments (Art. 43):

Self-assessments are possible for those high-risk AI systems which are not part of a regulated product in the context of the New Legislative Framework – except for biometric identification or categorisation systems, which may only self-assess if harmonised standards or common specifications were applied.

Conformity assessments must be carried out by an **assessment body** if the high-risk AI system is used for biometric identification or categorisation purposes, but does not conform to standards or common specifications. If the high-risk AI system is intended for use by law enforcement, immigration or asylum authorities, the conformity assessment must be carried out by the authority which supervises these institutions (Art. 63 para. (5)). If the system will be used by EU institutions, bodies or agencies, the European Data Protection Supervisor will carry out the assessment (Art. 63 para. (6)).

High-risk AI systems which are products or part of products requiring conformity assessments under the New Legislative Framework (Annex II, Section A) need to be **assessed according to the applicable legal framework** (Art. 43). In addition, the technical documentation needs to be examined by the authority responsible. In case the documentation provided is insufficient, the provider is obliged to provide further evidence or tests, and if necessary, access to the source code; the responsible authority may also test the system itself. If the data used to train the system does not conform to the requirements of this Regulation, the authority may ask the provider to retrain the system with appropriate data (Annex VII, point 4.3, 4.4, 4.5 and the fifth paragraph of point 4.6).

The European Commission may add new elements to the conformity assessment procedure if these become necessary by way of delegated acts. The Commission may also change procedures related to conformity assessments for high-risk AI systems used for the management and operation of critical infrastructure or for the administration of justice and democratic processes.

EU declaration of conformity (Art. 19 + 48)

After completing the conformity assessment, the provider needs to draw up a declaration of conformity before placing the system on the European market (Art. 19). This declaration must be retained for 10 years (Art. 48 and 50). For each system, the provider must provide one declaration of conformity identifying the system in an official EU language or the language required by the Member State (Art. 48). By drawing up the declaration of conformity, the provider assumes responsibility for the high-risk AI system's compliance. The declaration must contain (Annex V):

- Basic information about the **system** (name, type, identification details),
- Basic information about the **provider** or authorised representative of the provider (name, address)
- A **statement of responsibility**,

- A **statement confirming the high-risk AI system's compliance** with the AI Act (and other legislation, if applicable),
- References to **standards or common specifications** used for this system,
- Basic information about the **issue of the declaration** (place, date, name and function of signatory and on whose behalf the declaration was signed)

In case the high-risk AI system needs to undergo other conformity assessments, the provider only has to draw up one declaration of conformity which contains all of the information required by the AI Act and the applicable legislation. The European Commission may adopt delegated acts to amend the requirements for conformity declarations, should further elements become necessary over time (Art. 48).

Registration (Art. 51)

Providers of AI systems used for high-risk use cases (or their authorised representatives) need to **register their system** in an EU database for high-risk AI systems (Art. 51). This provision does not apply to AI systems which are products or part of products regulated by product safety legislation under the New Legislative Framework. The information which must be provided is specified in Annex VIII and comprises:

- All of the **information presented on the declaration of conformity** and a **copy of this declaration**,
- A **description** of the high-risk AI system and its intended purpose,
- The **market status** of the system **in every Member State**,
- Information about the **certificate of conformity** issued by the conformity assessment body and a digital **copy of this certificate**,
- **Instructions for use** (except for systems used for law enforcement, migration, asylum and border control management), and
- (Optionally) an URL for additional information.

CE marking (Art. 19 + 49)

Before placing the AI system on the European market, providers need to **affix a CE marking** to the high-risk system (Art. 19). The CE marking must be visible, legible and indelible. Since affixing a CE marking on software might prove challenging, providers have the option of affixing it to the packaging or the accompanying documentation. Next to the CE marking, the **identification number of the conformity assessment body** which certified the system needs to be displayed – also in promotional materials referring to the conformity of the high-risk AI system with the AI Act (Art. 49). The requirement to list the identification number of the conformity assessment body does not apply to high-risk AI systems which have undergone self-assessment by the provider.

Information and corrective actions (Art. 21, 22, 62 + 65)

In case any issues arise or the provider believes their system does not comply with this Regulation, the provider is obliged to undertake corrective actions, withdraw the high-risk AI system from the market or recall it. Regardless of which measures are taken, the provider must inform the affected distributors, importers and authorised representatives of these actions (Art. 21). Providers are obliged to inform the national competent authorities and (where applicable) the notified body which

issued the certificate for the system of any non-compliance regarding fundamental rights and any corrective action taken (Art. 22).

Art. 62 further specifies that providers are responsible for reporting serious incident or malfunctions that breach fundamental rights to the market surveillance authorities – immediately after establishing a causal link between the system and the incident or malfunctioning, and no later than 15 days after becoming aware of the problem. The European Commission will prepare guidance to comply with the requirements for reporting serious incidents and malfunctions within twelve months after the AI Act enters into force.

The provider is also obliged to **comply with requests for information** (including access to logs, if available) on the high-risk AI system by national competent authorities and authorities tasked with safeguarding fundamental rights (Art. 65). If market surveillance authorities establish that a risk to health, safety or fundamental rights remains unsolved, the provider must comply and **take corrective action** (Art. 22). Corrective action should be taken as appropriate to bring the system into compliance, and may include withdrawal or recall of the high-risk AI system (Art. 65).

Cooperation and demonstration of conformity (Art. 23)

Upon request by a national competent authority, providers need to cooperate with these authorities and provide them with all information and documentation necessary to demonstrate the conformity of the high-risk AI system with the AI Act. This includes access to logs upon reasoned request, if these are under their control (Art. 23).

Retention of documents (Art. 50)

Art. 50 obliges providers to retain the following documents for every high-risk AI system for ten years:

- technical documentation,
- documentation of the quality management system,
- documentation regarding changes approved by notified bodies,
- decisions and other documents issued by notified bodies and
- the EU declaration of conformity.

Obligations of importers

The AI Act defines importers as "any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union" in Art. 3 para. (6). For providers without the means to name an authorised representative within the EU, importers will have the crucial function of making their systems available in Europe.

As an importer, you are required to ensure that the provider has fulfilled her or his obligations under the AI Act. The duties of importers are specified in Art. 26 and boil down to checking documentation, providing information and complying with requests by authorities.

Importers are required to ensure the validity and availability of the **conformity assessment**, of the **technical documentation**, of the **CE marking** and the **documentation and instructions for use**. These

documents are essential for distributors and users to fulfil their obligations and importers have a special role in ensuring that high-risk AI systems from outside the EU conform to European product safety legislation (i.e., the AI Act).

The importer can only place high-risk AI systems on the market or put these systems into service if and when they conform with the requirements for high-risk AI systems – **systems which do not conform cannot enter the market or be put into service**. In case of risks to health, safety and fundamental rights, the importer must **inform the market surveillance authorities**.

Importers are also required to add their **name, trademark and contact details** on the high-risk AI system, its packaging or accompanying documentation, thus ensuring transparency regarding their role in the supply chain.

The importer is obliged to **comply with requests for information** (including access to logs, if available) on the high-risk AI system by national competent authorities and authorities tasked with safeguarding fundamental rights (Art. 65). If market surveillance authorities establish that a risk to health, safety or fundamental rights remains unsolved, the importer must comply and **take corrective action** (Art. 26). Corrective action should be taken as appropriate to bring the system into compliance, and may include withdrawal or recall of the high-risk AI system (Art. 65).

Obligations of distributors

Distributors are defined in Art. 3 para. (7) as "any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties". For smaller providers in Europe, distributors could potentially fulfil an important function of making their high-risk AI system available in countries other than the one they are established in if they lack the resources to expand into other national markets. Like importers, many of their obligations revolve around checking documentation, providing information and complying with requests by authorities. The obligations for distributors are set out in Art. 27.

As a distributor, you will need to ensure the validity and availability of the **CE marking** as well as the **documentation and instructions of use** and verify the **provider's and (if applicable) importer's compliance** with their obligations.

The distributor may only make high-risk AI systems available if and when they conform to the requirements specified in the AI Act – **systems which do not conform cannot enter the market or be put into service**. If the high-risk AI system poses a risk to health, safety or fundamental rights, the distributor must **inform the provider or (if applicable) the importer**.

If a high-risk AI system is discovered to be non-conforming with the requirements of the AI Act, the distributor shall take any **corrective actions** necessary to bring the system into conformity, to withdraw or recall it or to ensure that the provider, the importer or any relevant operator takes these corrective actions. If the high-risk AI system presents a risk to health, safety or fundamental rights, the distributor must **inform national competent authorities** of the non-compliance and any corrective actions. In case the user identifies a serious incident or malfunction and cannot reach the provider, the distributor must inform the market surveillance authorities of the Member State(s) in which the breach or malfunction occurred – immediately after establishing a causal link and in any case no later than 15 days after becoming aware of the incident or malfunction (Art. 62, based on

Art. 29 para. (4)). Distributors have to comply with reasoned **requests for information and documentation** with national competent authorities to **demonstrate conformity** of a high-risk AI system, and **cooperate on any actions taken** by these authorities. The distributor is obliged to **comply with requests for information** (including access to logs, if available) on the high-risk AI system by national competent authorities and authorities tasked with safeguarding fundamental rights (Art. 65). If market surveillance authorities establish that a risk to health, safety or fundamental rights remains unsolved, the distributor must comply and **take corrective action** (Art. 27). Corrective action should be taken as appropriate to bring the system into compliance, and may include withdrawal or recall of the high-risk AI system (Art. 65).

Obligations of users

The AI Act sets out a certain level of responsibility for users, which are defined as "any 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" in Art. 3 para. (4). The obligations of users are set out in Art. 29 of the Act and focus on using the high-risk AI system as intended and ensuring awareness of its risks.

Users need to use the high-risk AI system **according to the instructions of use** which need to be provided along with the system (please note: the instructions for use are not the same as the technical documentation, which does not have to be made available to users). If the user controls input data, the user needs to ensure that this **input data is relevant** considering the intended use of the system. Provided logs are under their control, the user has to **retain the logs** for an appropriate period of time considering the purpose of the high-risk AI system and the applicable legal obligations.

Based on the instructions of use, the user is obliged to **monitor** the high-risk AI system during operation and (where applicable) to conduct a data protection impact assessment. If the user becomes aware of **risks to health, safety or fundamental rights** as defined in Art. 65 para. (1), they need to inform the provider or distributor and suspend use of the system. In case of serious incidents or malfunctioning and interrupt the use of the system, the user needs to inform the provider or the distributor, if the provider cannot be reached.

How can I get my high-risk AI system certified?

As a **provider** or **authorised representative** of a provider, you can either certify your AI system or apply for certification with any conformity assessment body (also known as notified bodies). See above for more details on the requirements. Which certification procedure is necessary depends on the AI system. High-risk AI systems have to be re-certified whenever they are substantially modified, and in the case of self-learning systems, whenever changes occur that have not been pre-determined and specified in the technical documentation (Art. 43). The fees for conformity assessments will take into account the interests and needs of small-scale providers and be reduced proportionately to their size and market size (Art. 55).

Assessment based on internal control (Annex VI)

Self-assessments are possible for all **AI systems used in the specified high-risk areas**, with an exception for biometric identification and categorisation: there, self-assessments are only possible if you have applied either harmonised standards or common specifications (Art. 43). The conformity

assessment procedure based on internal control is specified in Annex VI: the provider must verify the **compliance of the quality management system** with Art. 17, examine the **technical documentation** to assess its compliance with the requirements in the AI Act, and verify that the design and development process of the high-risk AI system and its post-market monitoring are **consistent with the technical documentation**. Conformity assessment bodies are not involved in case of an assessment based on internal control.

Assessment by a notified body (Annex VII)

Assessments by notified bodies are necessary for all high-risk AI systems subject to **product safety legislation** under the New Legislative Framework and for **biometric identification systems** which have not applied harmonised standards or common specifications (Art. 43). Annex VII specifies the procedure for conformity assessments by notified bodies and focuses on the **quality management system**, the **technical documentation** and **compliance surveillance**. It sets out details regarding the **provider's application** and the **steps to be taken by the notified body**. Upon successful completion of the assessment, the conformity assessment body issues a certificate of conformity.

Biometric identification and categorisation systems intended for use by law enforcement, immigration or asylum authorities must be checked by either the data protection authority or those authorities tasked with supervising law enforcement, immigration or asylum authorities (Art. 43).

For high-risk AI systems to which other legislation under the New Legislative Framework applies, the conformity assessment is carried out by that body which usually approves product conformity (Art. 43). In addition to the requirements of the applicable legal act, some parts of Annex VII need to be considered: the **technical documentation** must be examined, further **information must be provided** if necessary (including the source code) and if the notified body refuses to issue a conformity certificate, it is necessary to **retrain the high-risk AI system**.

What about AI systems that are neither prohibited nor high risk?

While the main focus of the AI Act lies on high-risk AI systems, the Act defines two other categories of AI systems: prohibited systems, which we have discussed further above, and AI systems that need to offer a certain level of **transparency** to those affected by the systems – what we would call 'medium-risk' AI systems. What remains undefined by the AI Act are AI systems entailing low risk.

AI systems requiring transparency

In Art. 52, the AI Act sets out obligations for these three use cases. This list is conclusive, as no mechanism is foreseen for adding further use cases or obligations. Note that, as with high-risk AI systems, there is no right to object to or refuse interacting with an AI system: this means the AI Act does not give individuals the right to, for example, refuse to interact with a chatbot.

AI systems interacting with natural persons (Art. 52 para. (1))

If an AI system interacts with natural persons, as would be the case for chatbots, the **provider** must be transparent about the system's AI nature. The system must be designed and developed in a way which makes it **clear to anyone interacting with it that the system is an AI system**, unless it is already obvious from the circumstances and context of the use. Systems which are legally authorised to detect, prevent, investigate and prosecute criminal offences are exempted from this requirement, unless the system's purpose is intended for the public to report a criminal offence.

Emotion recognition or biometric categorisation systems (Art. 52 para. (2))

If an emotion recognition or biometric categorisation system is put into use, the **user** is responsible for **informing people exposed to the system of its operation**. Biometric categorisation systems legally authorised to detect, prevent and investigate criminal offences are exempted from this obligation.

AI-generated or –manipulated content (Art. 52 para. (3))

If an AI system generates or manipulates image, audio or video content in a way that may seem real, the **user** must **disclose that the content is artificial** and not, as might be supposed, real. This provision aims to counter the use of deep fakes for purposes of misinformation. AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences are exempted from this obligation. Another exemption exists in cases where the use of such content is necessary to exercise the right to freedom of expression and the right to freedom of the arts and sciences and appropriate safeguards for the rights and freedoms of third parties are in place.

Low-risk AI systems

The AI Act does not define any obligations for the development, market entry or use of AI systems which do not fall into the categories prohibited, high-risk or systems requiring transparency. The intention is to encourage the development and uptake of AI systems without placing undue regulatory burdens on providers or others. However, providers can choose to comply with codes of conduct (Art. 69), which we have described in more detail further below.

Who will be responsible for enforcing compliance with the AI Act?

In addition to the roles introduced for different operators of AI systems, the AI Act develops different roles for regulatory authorities at the national (or even international) and at the European level.

Notified bodies

The first level of monitoring is provided by independent **conformity assessment bodies** (so-called 'notified bodies') which are tasked with evaluating whether those high-risk AI systems which must be assessed by third parties comply with the requirements defined in the AI Act regarding **technical documentation** (plus supplements) and the **quality management system** (Art. 33, 43 and Annex VII). If the technical documentation and the quality management system fulfil all requirements, the notified body issues a **certificate of compliance** (Art. 44). Notified bodies are approved by the notifying authorities of each Member State. These notified bodies may be located in that Member State or elsewhere – even outside the European Union (Art. 39).

National competent authorities

As set out in Art. 59, every Member State should establish or designate independent authorities tasked with enforcing the AI Act. The Member State needs to ensure adequate financial and human resources to fulfil their obligations and dispose of a sufficient number of permanent staff with competences and expertise in artificial intelligence, data and data computing, fundamental rights, health and safety risks as well as existing standards and legal requirements. They may also provide advice and guidance on the implementation of the AI Act to local providers.

Among the competent authorities, there should be one **supervisory authority** which acts as **notifying authority** and **market surveillance authority**, unless administrative and organisational reasons give advantages to a Member State designating more than one authority (Art. 59). The supervisory authority is responsible for reporting to the European Commission on the outcomes of market surveillance activities on a regular basis and share information without delay that might be connected to the application of Union law on competition rules (Art. 63).

Notifying authorities

Notifying authorities act as **supervisors** for all organisations approved as notified bodies in a Member State (Art. 30). They shall be independent and impartial and will **assess, designate, notify and monitor notified bodies**. Member States also have the option of designating a national accreditation body as a notifying authority (Art. 30 para. (2)). Notifying authorities are tasked with ensuring that conformity assessment procedures are proportionate and do not contain unnecessary burdens for providers. Also, they must ensure that notified bodies take into account the size and structure of a provider, the sector in which it operates and the complexity of the AI system undergoing a conformity assessment.

Market surveillance authorities

Market surveillance authorities are responsible for monitoring the compliance of the product after it is placed on the market or put into use in the respective Member State. In case of **serious incidents or malfunctions**, the provider must report to the market surveillance authority, which will in turn inform the relevant public authorities (Art. 62). If it has reason to believe an AI system does not comply with the AI Act, the market surveillance authority may evaluate the system in question and, in case of non-compliance, define **measures to remedy the non-compliance** or request the **recall or withdrawal of the system** from the market (Art. 65, 67 and 68).

Market surveillance authorities also have the power to issue a **derogation** from the obligation to obtain certification for a high-risk AI system – specified in Art. 43 – for a limited time, and only for reasons of public security, protection of life and health of persons, environmental protection and protection of key industrial and infrastructural assets (Art. 47).

According to Art. 63, Member States should designate the authority enforcing the applicable product safety legislation, if the legal acts in Annex II apply, as market surveillance authority for those AI systems pursuant to the AI Act. For biometric identification in the context of law enforcement, law enforcement or migration-related AI systems, the data protection authority or that authority which supervises the activities of law enforcement, immigration or asylum authorities should be designated as market surveillance authority.

Other national authorities

Member States can submit a list of authorities which are competent to enforce **obligations relating to fundamental rights** (Art. 64(3-6)). The list of these authorities must be publicly available. These authorities may **request and access any documentation** created or maintained for the purposes of this Regulation and must inform the market surveillance of their Member State of any requests made. In case the existing documentation is insufficient to determine whether a violation of fundamental rights may have occurred, these authorities may ask the market surveillance authority to **organise testing** of the high-risk AI system in question, which shall take place with close

involvement of the authority in question and in a reasonable time period. Any documentation or information obtained through these provisions must be treated confidentially.

Artificial Intelligence Board

The supervisory body will also represent its Member State in the **Artificial Intelligence Board** (Art. 57). The aim of the Artificial Intelligence Board is to advise and assist the European Commission by contributing to effective cooperation of national supervisory authorities and the Commission, coordinating and contributing to guidance and analysis of the Commission and national supervisory authorities and others on emerging issues, and assist the Commission and national supervisory authorities in the consistent application of the AI Act. Together with the Commission, the Board will encourage and facilitate voluntary codes of conduct related to (for example) environmental sustainability, accessibility for persons with a disability, stakeholder participation in the design and development of AI systems, diversity of development teams (Art. 69). In addition, the Artificial Intelligence Board will offer a framework for national competent authorities overseeing regulatory sandboxes to coordinate and cooperate their activities (Art. 53).

European Commission

The AI Act gives the European Commission a multitude of tasks. It shall, for instance, assign an identification number to notified bodies and make the list of assigned numbers publicly available (Art. 35). If it has reason to doubt the compliance of a notified body, it will investigate the case and, if non-compliance is proven, will request the notifying authority to take corrective measures, including withdrawal of notification (if necessary) by way of an implementing act (Art. 37). The Commission will further ensure coordination and cooperation of the notified bodies in the form a sectoral group, in which all bodies will participate (Art. 38).

One of the keys of the certification process rests on the availability of harmonised standards which providers can apply to their systems. In case these harmonised standards are not available or insufficient, or specific safety or fundamental rights concerns need to be addressed in addition to existing standards, the Commission can adopt common specifications by way of implementing acts after consulting stakeholders in the relevant sectors (Art. 41). The European Commission will also set up a database for high-risk AI systems where providers need to register their systems before placing them on the European market (Art. 60).

In case an operator does not take corrective action to achieve compliance with the AI Act, and in case the market surveillance authority takes measures to restrict the availability of the system (Art. 65 para. (5)) to which a Member State or the European Commission raises an objection, the Commission will consult with the Member State and the operator(s) concerned and decide on whether the measure is justified (Art. 66). If an AI system presents a risk despite being compliant with the requirements, the Commission will evaluate the measures taken by the market surveillance authority (Art. 67).

The Commission will also chair the Artificial Intelligence Board, convene meetings and prepare the agenda as well as providing administrative and analytical support for the activities of the Board. This includes facilitating exchanges between the Board and other Union institutions (Art. 57) and between national competent authorities (Art. 59). Together with the Artificial Intelligence Board, the Commission will encourage and facilitate voluntary codes of conduct related to environmental sustainability, accessibility for persons with a disability, stakeholder participation in design and

development of AI systems and diversity of development teams (amongst others). These codes of conduct should be based on clear objectives and key performance indicators and take into account the specific interests and needs of small-scale providers and start-ups. Together with the Member States, the European Commission will also encourage and facilitate voluntary codes of conduct which apply the requirements for high-risk AI systems to other AI systems (Art. 69).

Yikes, regulation. How much do I have to pay if I do not wish to comply?

Penalties for non-compliance as specified in Art. 71 vary according to size and sector of the **operator**, but are by no means insignificant. Please note: any person or organisation responsible for an AI system in any role is considered an operator, but Member States need to lay down rules on whether and to which extent public authorities and bodies in that Member State will be subject to fines.

Special consideration will also be taken of the nature, gravity and duration of the infringement and its consequences and whether administrative fines have been applied by other market surveillance authorities for the same infringement.

Non-compliance with the prohibition of AI systems or non-compliance with the requirements for data governance may be fined with up to **30 000 000 Euro (or up to 6% of the total worldwide annual turnover for companies)**.

Non-compliance with other obligations and requirements set out in the AI Act may lead to fines of up to **20 000 000 Euro (or 4% of the total worldwide annual turnover for companies)**.

Supplying incorrect, incomplete or misleading information to notified bodies and national competent authorities leads to fines of up to **10 000 000 Euro (or 2% of the total worldwide annual turnover for companies)**.

Fines for non-compliance of Union institutions, agencies and bodies are significantly lower and will be set by the European Data Protection Supervisor (Art. 72). In these cases of non-compliance, the nature, gravity and duration of the infringement and its consequences, the cooperation with the European Data Protection Supervisor to remedy the infringement and any previous infringements by the institution in question will be taken into consideration.

Non-compliance with the prohibition of AI systems or non-compliance with the requirements for data governance may be fined with up to **500 000 Euro**.

Non-compliance with other obligations and requirements set out in the AI Act may lead to fines of up to **250 000 Euro**.

Yay, regulation. Which opportunities does the AI Act open for my AI system on the European market?

For providers, importers or distributors, the AI Act brings legal certainty when making an AI system available on the European market. The same goes for users, which may be more likely to adopt AI systems if they can rely on specific procedures which are considered safe. For providers of

unregulated AI systems, voluntarily applying codes of conduct may inspire trust in their procedures and products. This may especially be the case for small-scale providers and start-ups.

In addition, the AI Act specifies a set of measures which are meant to support innovation in the development of AI systems.

Regulatory sandboxes (Art. 53 + 54)

Regulatory sandboxes are a relatively new concept aiming to provide a **controlled environment for testing new technologies**. The AI Act allows for the establishment of regulatory sandboxes by one or more Member States or the European Data Protection Supervisor where competent authorities shall offer time-limited supervision and guidance for development, testing and validation before making these available on the market. In case of any significant risks to health, safety and fundamental rights, mitigating measures must be taken immediately or the development and testing process will be suspended until the risk is mitigated. The liability of participants in the regulatory sandbox in case of harm to third parties remains intact (Art. 53).

The AI regulatory sandboxes will also allow providers to **process personal data** lawfully collected for other purposes under specific conditions and only with appropriate safeguards in place. The sandboxes should only be available for applications developed in the public interest (related to law enforcement and security, to public safety and health or to environmental protection and sustainability) and only if the processing of data is necessary to comply with the requirements for high-risk AI systems and anonymised, synthetic or other non-personal data cannot ensure compliance. Access to the personal data which is processed in the sandbox has to be highly restricted, logs of the processing must be retained for the duration of participation and one year after it ends and the data itself is deleted once it reaches the end of its retention period or the participation in the sandbox ends. Throughout the duration of the sandbox, effective monitoring mechanisms need to be in place to detect and mitigate any risks to fundamental rights, and the processing of personal data in the sandbox cannot lead to measures or decisions which affect the data subjects. Finally, the process and rationale behind training, testing and validation must be described and made part of the technical documentation together with the testing results. In addition, the authority overseeing the sandbox will publish a short summary of the AI project, its objectives and expected results on its website.

Small-scale providers and users (Art. 55 + 69)

Small and medium enterprises form an important part of the European economy and have an important role in developing new technologies. To support small-scale providers, the Member States will provide small-scale providers and start-ups with **priority access to regulatory sandboxes**, provided they are eligible. They are also obliged to **raise awareness** about the AI Act in a manner that is tailored to the needs of operators and (where appropriate) establish a point of contact to **provide guidance and answer questions** regarding the implementation of the AI Act. Similarly, the fees for conformity assessment shall be reduced for small-scale providers proportionately to their size and market size (Art. 55).

When encouraging and facilitating the drawing up of codes of conduct, the Commission and the Board will take into consideration the interests and needs of small-scale providers and start-ups (Art. 69). This provision applies only to codes of conduct related to requirements other than those defined for high-risk AI systems.

Advice and guidance (Art. 59)

Member States may establish a point of contact to communicate with operators and national competent authorities may provide guidance and advice on the implementation of this Regulation (also to small-scale providers).

Codes of conduct (Art. 69)

The AI Act defines legal requirements for certain AI systems, but it also aims to encourage the application of voluntary codes of conduct to AI systems which do not face specific obligations. Codes of conduct can be developed by providers of AI systems, by organisations representing them or by both. Users and interested stakeholders as well as their representative organisations may be involved in drawing up the codes of conduct. The codes of conduct should focus on the intended purpose of AI systems and may cover one or more systems.

Two types of codes of conduct will be encouraged and facilitated by the European Commission. On the one hand, the Commission together with the Member States will promote the development of **codes of conduct based on the requirements for high-risk AI systems** defined in the AI Act.

On the other hand, the Commission together with the Artificial Intelligence Board will promote **codes of conduct for topics which are not regulated by the AI Act**, such as codes of conduct for environmental sustainability, accessibility for persons with a disability, stakeholder participation in the design and development of AI systems or diversity of development teams. These codes of conduct will be based on clear objectives and key performance indicators which allow for measuring the achievement of the specified objectives. For these codes of conduct, specific interests and needs of small-scale providers and start-ups should be taken into account.

Anything else I should know?

The AI Act contains several special provisions for credit institutions or applications related to credit and finance. We have not gone into detail on these in the briefing and would recommend a thorough reading of the legal text.

Researchers, journalists and civil society activists looking into the impact of AI systems may find the database of high-risk AI systems offered by the European Commission to the general public to be a valuable tool, even though the information provided is rather limited (e.g. no information on the users of high-risk AI systems). Of course, this depends on how the database is designed: a user-friendly design would go a long way towards making the use of automated systems more transparent. Likewise, regulatory sandboxes will publish short summaries of the projects enrolled on the website of the authority overseeing the sandbox, including details on the AI system's objectives and expected results.

AI development greatly benefits from open-source contributions. The AI Act applies to AI systems which are made available under a trademark or logo, whether for payment or free of charge. As a developer working in the field of AI and interested in making her knowledge available to others, it would be advisable to specify the intended use of the AI system and adding that the system cannot be used for purposes that are deemed prohibited, high-risk, or entail other obligations for providers

under the AI Act. Aside from the legal obligations, we would however encourage engaging with the specifications for technical documentation, as we believe these include good practices which will make your AI system easier to understand, evaluate and use.

Recommendation algorithms on social media platforms, despite being one of the most commonly encountered types of AI system, will not be regulated in the current version of the AI Act - similarly, AI systems used to flag or delete content from social media platforms will not be regulated. Search algorithms, which even those who do not use social media platforms are exposed to on a regular basis, will not face obligations under this version of the regulation. Aside from these applications, pricing algorithms also fall outside the scope of the AI Act. None of these systems are regulated per se in the Digital Services Act or the Digital Markets Act, as these legislative proposals focus more on the conduct of companies and rights of end users and business users when engaging with services provided by digital platforms or gatekeepers, respectively.