March 15, 2023

Artificial Intelligence Act	
Status:	**PENDING** Commission's original proposal 21 April 2021 Compromise text 25 November 2022
About:	Harmomized rules for the placing on the market and using of AI systems (other than for purely personal use), through 1) prohibiting certain AI practices; 2) providing specific requirements for high-risk AI systems and operators of such systems; 3) providing transparency rules for certain AI systems; 4) measures to support innovation.
Applies to:	Developers and service providers of AI systems, also those located outside of Union of output produced by the system is used in Union; distributors of AI systems; those who put their trademarks on AI systems; importers; distributors; as well as users of AI systems.
"AI system" (art 3(1))	Means software or service systems having learning, reasoning and modelling capabilities characteristic to artificial intelligence and having been designed to operate with elements of autonomy (EU Commission may later adopt a more technical definition). A system that uses rules defined solely by natural persons to automatically execute operations should not be considered an AI system.
Prohibited practices (art 5)	Certain AI practices shall always be prohibited, including AI systems that - deploy sublimal techniques beyond person's perception distorting human behaviour and causing physical or psychological harm, - exploit vulnerabilities of specific group of persons due to their age, disability or social or economical situation, - make behavioral classification of persons, with the social score leading to unfavorable treatment of persons in social contexts unrelated to the original context or otherwise to treatment that is disproportionate to the behaviour, - use of real-time remote biometric identification in public by law enforcement authorities for law enforcement, unless exception applies
High-risk AI systems (art 6; Annex II)	AI system will be considered as high-risk, where 1) the AI system is itself a product subject to EU harmonized legislation (Annex II) or is a safety component of such product, and is required to undergo a third-party conformity assessment for placing on the market, or 2) the systems is any of the following (Annex III): o remote biometric identification systems o safety components of critical digital or physical infrastructure

	○ systems determining admission to education, and systems evaluating learning outcomes ○ recruitment systems, employee performance monitoring systems ○ access to public benefits or services ○ evaluation of creditworthiness of natural persons (exception for systems provided by SME companies) ○ analysis relating to life and health insurances (exception for systems provided by SME companies) ○ various uses in law enforcement, including applying laws, and border control/migration Annex III may be later amended by Commission where any other AI system is considered to pose similar risk of harm to health and safety or impact on fundamental rights. AI systems that only have an accessory role in the systems described above are not considered high-risk systems. EU Commission will later provide guidance (through implementing acts) on circumstances that are considered accessory.
”General purpose AI systems” (art 4a)	EU Commission will later provide guidance (through implementing acts) on how the requirements for high-risk AI systems will be applied for general purpose AI systems that may be used as (components of) a high-risk AI system. General purpose AI system means software/system that performs generally applicable functions that can also be used in AI systems. Requirements for high-risk AI systems does not apply for general purpose AI systems, if the vendor has excluded use of the system in all high-risk uses in the product/service documentation, unless.
Risk management system (art 8)	In relation to high-risk AI systems, a risk management system for identification, analysing and mitigating known or foreseeable risks must be maintained. Risk management system must give specific consideration to impacts on persons under age of 18.
Data and data governance (art 10)	Training data sets must meet quality criteria such as having appropriate statistical properties. Data must be examined in view of possible biases leading to discrimination. For that purpose, also special categories of data can be processed.
Technical documentation (art 11)	Technical documentation must be in place before the system is placed on the market. Documentation must demonstrate compliance with the regulation. Annex IV sets out documentation requirements in detail (documentation criteria is somewhat looser for SME companies).
Record-keeping (art 12)	High-risk AI systems must enable appropriate logging of relevant events.

User information (art 13)	High-risk AI systems must be accompanied with user information specifying, among other, characteristics, capabilities and limitations of the system.
Human oversight (art 14)	High -risk AI systems must have interface for being effectively overseen (and intervened, if needed) by a natural person. Human oversight is especially required where a residual risk has been identified in the use of system that may not be limited by other means.
Cyber security (art 15)	High-risk AI systems must have appropriate level of accuracy, robustness and cybersecurity throughout time of use.
Obligations for providers of high-risk AI systems (art 16)	Providers of high-risk AI systems must have a quality systems in place that is documented in written policies, procedures and instructions. Documentation must be retained for 10 years. Provider must carry out conformity assessment of the quality system and **draw up an EU declaration of conformity** to be fixed in the product or its documentation.
Obligations of users	Users of high-risk AI systems must use the system in accordance with its instructions of use, and arrange appropriate human oversight and monitoring of the use of the system. Use of high-risk AI systems requires in most cases data protection impact assessment (DPIA) to be made under the GDPR.
Registration	Providers of high-risk AI systems must register themselves in the EU database. The information in the database is public.
Reporting of serious incidents	Providers of high-risk AI systems shall report any serious incidents to the marker surveillance authorities in the relevant member state. Notification must take place immediately but in any event not later than 15 days after becoming aware of the incident.
Transparency (art 52)	Providers must ensure that all AI systems are developed in such a way that natural persons are informed in a clear manner that they are interacting with an AI system. Users who manipulate content like images to generate content that resembles an existing person (deep fake), must disclose that the content has been artificially manipulated.