2021.AI

The EU's Artificial Intelligence Act

Understand the EU regulations
and which actions to take

Table of Contents

FOREWORD

The EU's Artificial Intelligence Act marks the end of more than 3 years of work in which 2021.AI has proudly taken part in. We are pleased to see the outcome, and we would like to share perspectives and some proposed actions with you.

From **2021.AI** we foresee an initial challenge to be precise on when a model falls into the high-risk category, but with more work and examples, this will be solved before the Act will be enforced in 2023.

More importantly, we believe the question is how we can ensure a proper solution to support all organizations who use or intend to use models which fall into the high-risk category. The largest organizations will build, or in most cases buy appropriate solutions and they can afford this. But what about Europe's SME (Small Medium Enterprises) segment, how can we manage this additional governance challenge? Europe's SME segment is in many cases already challenged and stretched on resources to **develop** and **operate** AI. Now, adding **governance** is not helping the adoption of AI in the EU. Also, in this paper, we will share the EU's estimated governance cost model per year. This number is high and too high for most SMEs.

In the act it is very important to note the definition of what models/systems are covered: *"(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference, and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods."*

This definition is broad and opens up for all types of models and systems that contain such models. Many systems will now and in the future have some type of model which corresponds to the EU definition.

From **2021.AI** we have been very pleased with our work with the EU in the last 2 years, and not least our continued work in the ETAPAS project where the scope is extended to include all disruptive technologies. 2021.AI wants to ensure a governed and compliant acceleration of the implementation of AI and other disruptive technologies, this to improve efficiency, reduce waste and at large make a positive impact with AI.

Mikael Munck

CEO and Founder of 2021.AI

THE EU'S AI ACT

Introduction

On April 21, 2021, the European Commission announced its comprehensive proposals for the regulation of artificial intelligence (AI). The announcement has already generated much interest, with a focus on how it will affect technological companies that develop AI systems and possible innovation roadblocks. Therefore, it is a must to ensure that senior executives understand the essentials of this new regulation together with its organizational impact.

The most important considerations rely on understanding the different levels of risk categorization, comprehension of the new rules and prohibitions from a user and provider perspective, monitoring and tracking the AI risk level over time, the incorporation of the new regulations in national legislation, awareness of fines up to 6% of a company's annual global turnover. The prevention of harm to individuals is the key objective which underpins the regulation. The EU Commission considers that harm may arise both physically, through AI systems being unsafe, and in relation to the risks caused to individuals' fundamental rights, such as privacy and the right to non-discrimination.

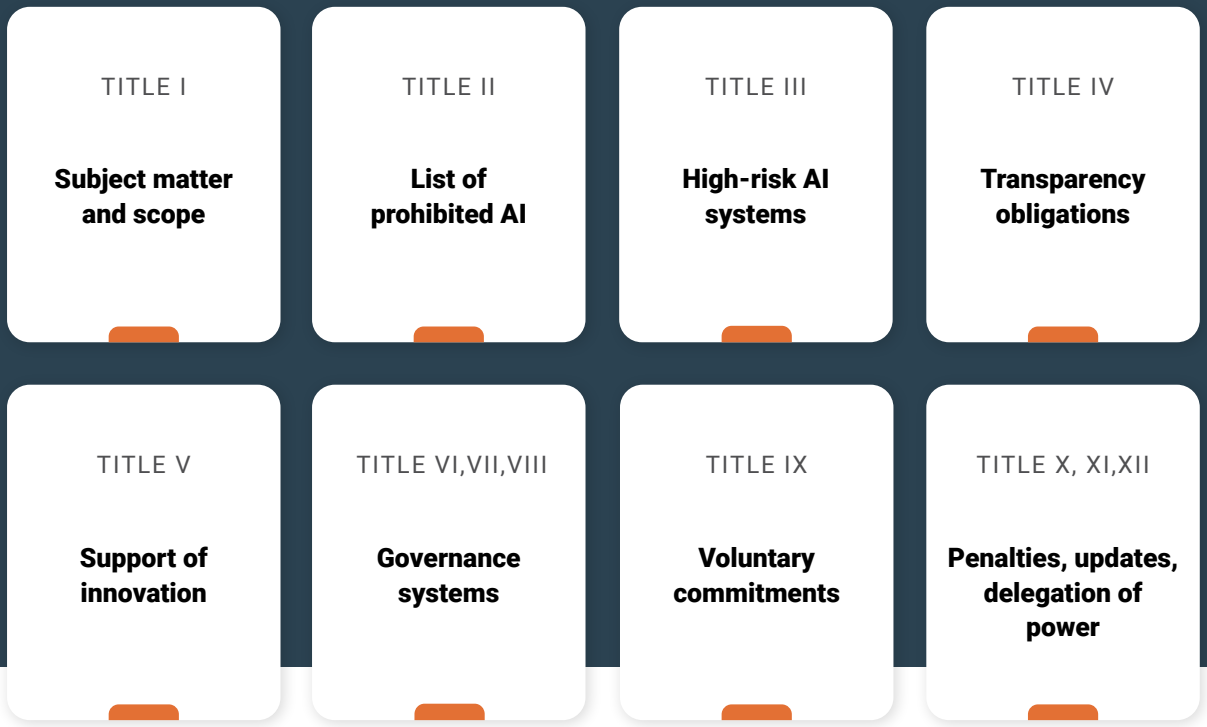
In this document, we will summarize the key points of the proposed **European Artificial Intelligence Act.** We will mention the challenges that we foresee arising from the proposal and provide suggestions on how to overcome these challenges.

SECTION 1

The Titles of the Act

This proposal supports the goal of pushing for safe development of AI and emphasizes the risks involved with the utilization of such technology. The proposal reinforces the intention of building a trustworthy ecosystem by suggesting a legal framework for responsible AI.

The framework should guarantee that AI systems within the EU comply with security and respect of the existing law on fundamental rights and the Union values; ensure legal certainty to facilitate investment and innovation in AI; stimulate governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems and facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation. The act consist of 12 Titles which are illustrated below:



Subject matter and scope

TITLE I : Defines the scope of application of the new rules. These cover the placing on the market, putting into service, and the use of AI systems.

List of prohibited AI

TITLE II: Lists and describes all the AI systems which are considered unacceptable as contravening EU values, for instance, by violating some fundamental rights.

High-risk AI systems

TITLE III: Contains specific rules for AI systems that create a high risk. The classification of an AI system as high-risk is based on the intended purpose of the AI system and will be covered in later parts of this document.

Transparency obligations

TITLE IV: Is about transparency obligations for systems that interact with humans, are used to detect emotions or determine association with (social) categories based on biometric data, or generate or manipulate content.

Support of innovation

TITLE V: Contributes to the objective to create a legal framework that will not hinder innovation.

Governance systems

TITLE VI: Sets up the governance systems at EU and national levels.
TITLE VII: Aims to facilitate the monitoring work of the Commission and national authorities.
TITLE VIII: Sets out the monitoring and reporting obligations for providers of AI.

Voluntary commitments

TITLE IX: Concerns a framework to encourage providers of non-high-risk AI systems to apply the requirements of high-risk systems voluntarily.

Penalties, updates, delegation of power

TITLE X: Sets out rules for the exchange of information obtained during the implementation of the regulation.
TITLE XI: Sets out rules for the exercise of delegation and implementing powers.
TITLE XII: Contains an obligation for the Commission to assess regularly the need for an update of Annex III and to prepare regular reports on the evaluation and review of the regulation.

SECTION 2

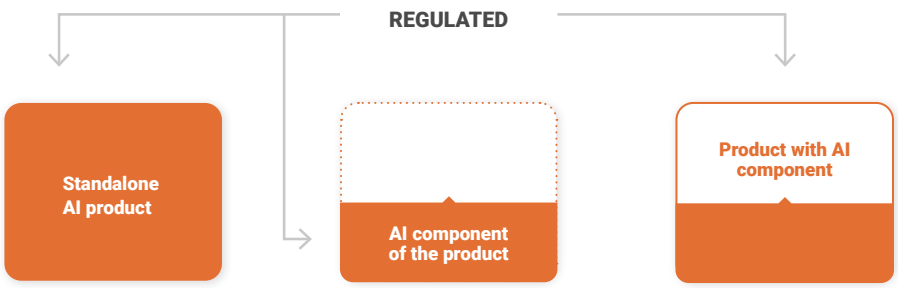
Who Is Impacted

The EU wants to lead the way with responsible AI. The new regulation and the commission have put forward an entirely new body of law, which intends to place ethical issues such as bias mitigation, algorithmic transparency, and human oversight of automated machines at the forefront of the regulation. The framework promises to have the same profound impact on the use of AI as the EU General Data Protection Regulation (GDPR) has had on personal data.

The EU did not lead the world in AI breakthroughs, but being a pioneer in regulating and ensuring human centered AI development is something that can give the EU an edge on AI development.

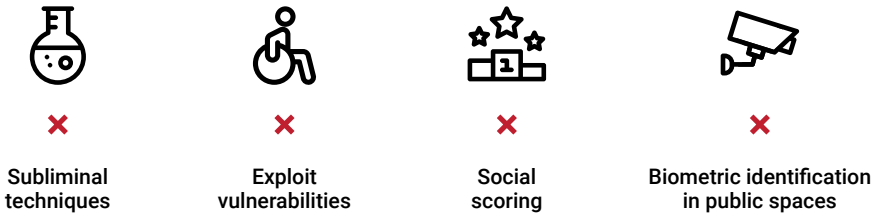
The question that arises is, who is impacted by this regulation? The short answer is that most are. It is very likely that the new EU regulations will affect everyone's business if it uses AI and if it is related to the EU in some sort of way.

Any company based in, or operating in the EU, that is working with AI or using a component with AI embedded is impacted by this regulation. Even if the company is not developing an AI system itself, if they are using systems that have an AI component present they are subject to adhere to the new rules.



The AI systems being used by companies fall into one of three categories. These categories are: prohibited, high risk, or low risk.

If a system is prohibited then there are only very slim avenues to continue its use. There is a process where it could be approved through the judicial system, where public and governmental bodies can argue for justified use. Prohibited systems include systems that exploit vulnerabilities, use subliminal techniques, calculate social scores, and biometric identification systems in public areas.

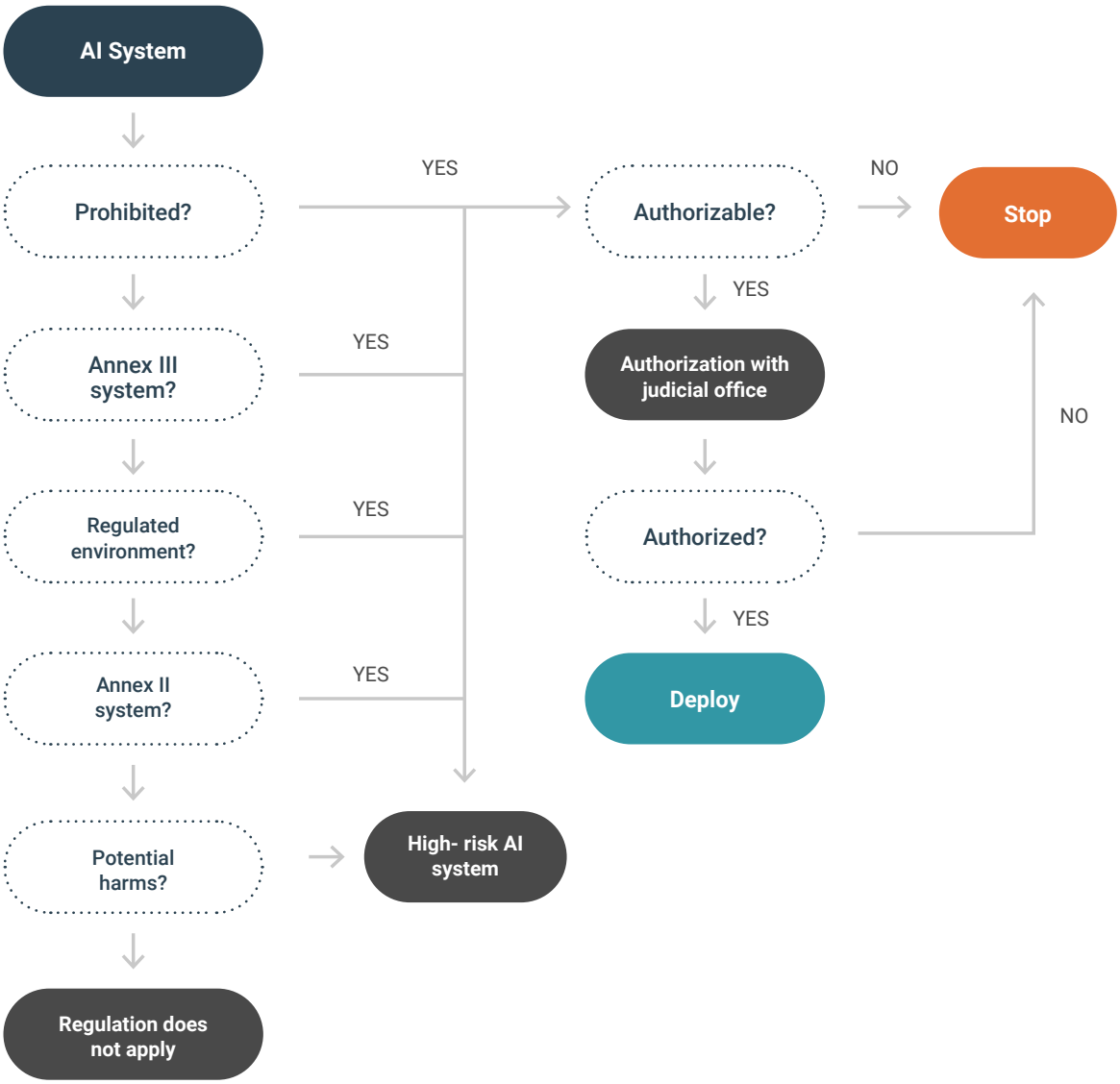


If the AI system is not prohibited then it can fall into the high-risk category. The list of high-risk systems is mentioned in Title III, Annexes II, and III of the regulation. The Commission provides criteria (see Article 6) to help understand whether AI systems fall into the high-risk category based on existing EU product safety legislation (listed in Annex II) or systems explicitly listed in Annex III (this list will be updated annually). Annex III provides a non-exhaustive list of some examples of high-risk AI systems:

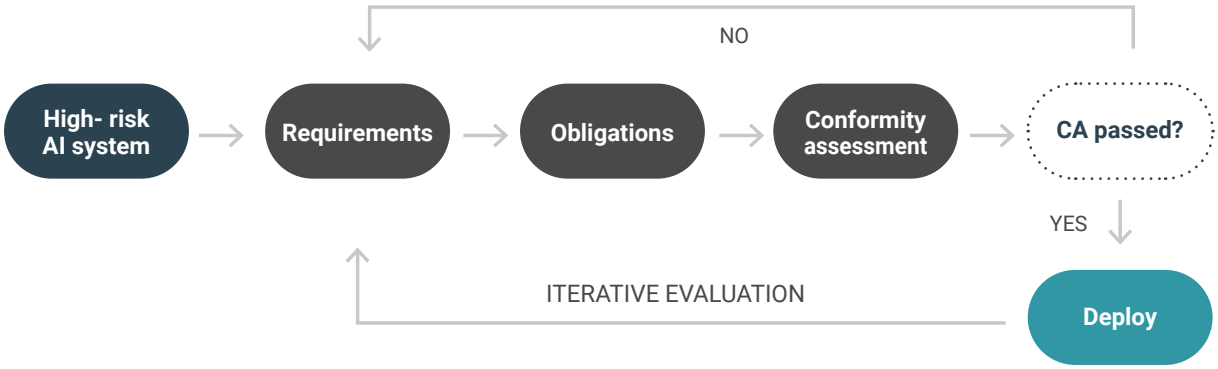
- **Critical infrastructures** (e.g. transport), that could put the life and health of citizens at risk;
- **Educational or vocational training**, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- **Safety components of products** ((e.g. autopilots or parking assistance);

- **Employment, workers management, and access to self-employment** (e.g. CV-sorting software for recruitment procedures);
- **Essential private and public services** (e.g. credit scoring denying citizens opportunity to obtain a loan);
- **Law enforcement that may interfere with people's fundamental rights** (e.g. evaluation of the reliability of evidence);
- **Migration, asylum, and border control management** (e.g. verification of the authenticity of travel documents);
- **Administration of justice and democratic processes** (e.g. applying the law to a concrete set of facts).

But how to know where your system belongs if it is not on the list? We have illustrated this in the following graphical guide:



Note: the figure describes a process one can follow to see whether the regulation applies to an AI system or not. It is a flow diagram starting at the upper left corner and asking questions on the way. Depending on the answers to the questions, one gets to either a green deployment stage or to a red stop stage.



Organizations that procure high-risk AI systems from third-party vendors are also subject to the new rules. These rules are underpinned by the expectation that the user adheres to and monitors operational performance in accordance with a set of technical instructions that will be developed by the provider.

Providers based in non-EU countries, such as the United States, will be subjected to the regulation's requirements if they make their AI system available in the EU. Similarly, and perhaps more significantly, the law will also apply to both providers and users of AI systems where the "output" of that system is used in the EU. In our perspective, this condition has the potential to catch a significant number of additional organizations that have no commercial presence in Europe.

For AI systems that are neither prohibited or deemed to be high-risk, the commission has taken a more pragmatic and light-touch approach. Providers will be expected to inform individuals when they are interacting with AI systems unless it is obvious. However, neither they nor the users will be expected to provide detailed explanations about the nature of the algorithms or how they operate. In other words the users are alone with the actual decision and with the selection of the approach. From our experience we recommend organizations to look into this and create a code of conduct because it will on one side fulfill the recommendation of the commission and on the other hand, people at the organization will start to look into this and define their own standards which is an active approach that should be preferred.

> *So there are no regulatory requirements, if not high risk, but here there is a recommendation: you should develop your own Code of Conduct - to get public and regulatory approval.*

SECTION 3

What You Should Be Aware Of

The European Commission will release a vital policy package, which will reflect the proposal of the regulation of AI that is being analyzed. This will be an important step towards a more clear definition of a comprehensive regulatory framework for AI and will include the final decisions made around AI regulation. It will consist of essential components seeking to lay down harmonized rules on AI defining high-risk applications, regulatory obligations for providers of AI systems, the post-market surveillance of AI, and the conformity assessment of high-risk AI applications[1]. Ultimately, the law revolves around assessments of compliance costs generated by the projected regulation on AI systems.

We strongly believe that starting now, and taking an agile approach will yield great savings in the long run. The alternative is putting all high risk models out of production and then redeveloping them from scratch - which is extremely timely and costly.

3.1. The Law

The new law sets out to regulate AI Use Cases in an ethical and trustworthy manner with a risk-based approach. High-risk AI systems will have to comply with several safety components and acquire a CE marking and process indicating a product fulfills the requirements of the relevant Union legislation. To affix a CE marking on an AI system, five compulsory steps need to be followed[2]. These steps concern important assessments such as determining whether an AI system is classified as a high-risk system, if you can ensure both an adequate QMS (Quality Management System) and if a conformity assessment procedure is in place all resulting in affixing

1 European Commission (2021). *Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. P. 2

2 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* p. 33

a CE marking and signing a declaration of conformity[3]. The purpose is to ensure high-quality training, validation, and testing of data while also establishing proper documentation and design logging features like traceability and auditability[4]. This is to ensure appropriate transparency and human oversight. These features are enabled by measures built into the system, ensuring robustness, accuracy, and cybersecurity.

The purpose of the law is to put forward regulatory demands empowering the common twin objective of harnessing the full power of AI, while also addressing the risks associated with the technology[5]. Moreover, the goal is to facilitate the development of an ecosystem of trust enabled by a legal framework on how to achieve ethical and trustworthy AI.

3.2. Reasoning and Objectives

The Union strives for further technological development and highly recognizes the value and opportunities AI brings with it. The Union further describes it as a fast-evolving family of technology that can bring with it a broad spectrum of both economic and societal benefits[6]. However, with the opportunities AI enables, new risks and negative consequences can be highlighted. The EU is therefore committed to strive for a well-balanced approach, not letting the rapid technological development with AI run its course without laying down harmonized rules and a legal framework from which the technology should operate. With proper oversight, ensuring trustworthy and ethical AI, the union feels confident that users will embrace AI as a technology, also inspiring businesses to further develop within the area.

Being at the forefront of this fast-evolving family of technology, with a well-functioning European market for AI, the Union strives to be a global leader of trustworthy and ethical AI by equally addressing both benefits and risks. The ambition stems from the importance of ensuring European citizens' rights are fully respected and as a result, the new AI act sets out to accomplish that through a coordinated approach on the human and ethical implications AI brings with it[7].

3.3. Public opinions

The new AI Act and the overall proposal is broadly based on a wide array of public opinions. An online public consultation consisting of multiple major stakeholders was launched on 19 February 2020, ending 14 June 2020. In short, 1.215 contributors in the shape of companies, business organizations, research institutions, and public authorities, gave valuable insights on the topic[8].

In 2020, the European Commission published a white paper regarding AI in the EU. The overall public opinion in response to this paper confirmed that there was a need for action. Concerns about legislative gaps were expressed and the need for new

3 Sioli, L. (2021). A European Strategy for Artificial Intelligence [PowerPoint slides]. Digital Industry DG CNECT, European Commission. https://www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf (Slide 10)

4 A European Strategy for Artificial Intelligence [PowerPoint slides]. Digital Industry DG CNECT, European Commission. (Slide 11)

5 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.1

6 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.1

7 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.2

8 European Commission (2018). *Commission Staff Working Document: Proposal for a Regulation of the European Parliament and of the Council:* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0052%2801%29

legislation was confirmed. The majority of stakeholders wished to avoid duplication, conflicting obligations, and overregulation, with the AI Act being technology-neutral with a proportionate regulatory approach. For example, tailoring the regulatory requirements to an organization's size and risk profile. Therefore, all stakeholders expressed a positive attitude towards the risk-based approach as opposed to a blanket regulation of all AI systems[9]. This in conjunction with the positive attitude towards the enforcement models concerning the ex-ante risk self-assessment and the ex-post enforcement for high-risk AI systems, has resulted in a large majority of the contributors in the online public consultation being in favor of the need for action.

The immediate benefits of starting early will not always emerge rapidly, but early action will help build trust for your organization. Customers and other outsiders will be aware that you have set yourself up for success and have done everything to prevent a negative event.

3.4. Penalties and fines

In accordance with Article 71 (Penalties), it is up to the member states to lay down rules on penalties including administrative fees and to confirm proper and effective implementation of such. In accordance with the results of the online public consultation, the penalties provided will take into account the size of the organization and its economic viability[10]. Nevertheless, the penalties set in place by the members' taxes must be effective and proportionate, and the member states are solely responsible to disclose exact rules and measures and notify the commission of any other amendments affecting them.

Firstly, infringements upon Prohibited Practices (Article 5[11]) and Data & Data Governance (Article 10[12]) will be subject to administrative fines of up to 30 000 000 EUR or, if the offender is a company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher[13].

Secondly, the non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher[14].

Lastly, the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher[15].

Fines can pile up to 10 - 30 Mio. EUR or 2%-6% of its worldwide annual turnover.

9 *Commission Staff Working Document: Proposal for a Regulation of the European Parliament and of the Council* P. 8

10 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.82

11 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.43

12 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.48

13/14/15 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.82

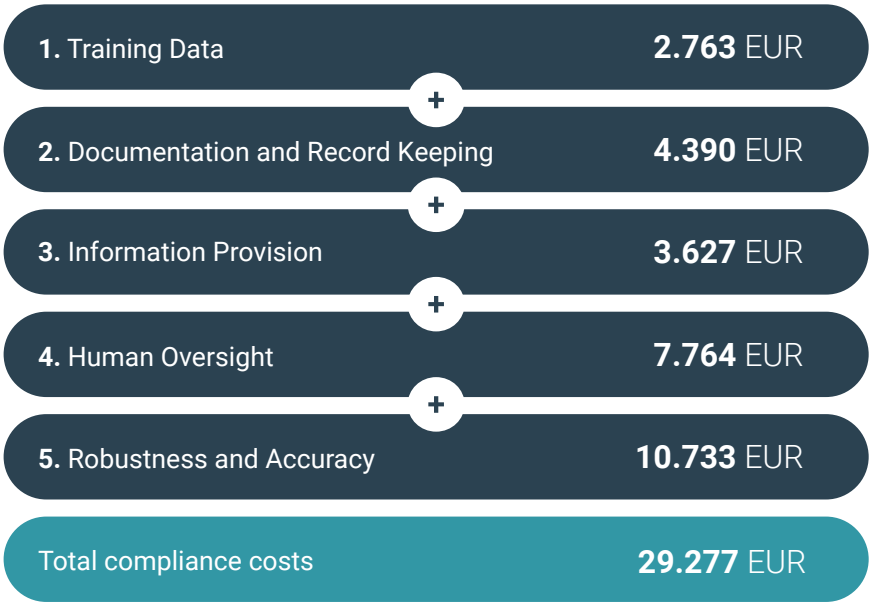
Each member state is equally responsible to ensure clear communication of penalties in full compliance with the terms and conditions set forward in the regulations, while also ensuring efficient implementation and enforcement of set regulations.

3.5. Assessment of the compliance costs

With the proposed AI act, an assessment of compliance costs is provided as a cost estimation of administrative burdens and detailed compliance costs. The cost model is developed by the Federal Statistical Office (FSO) from the German government[16]. Overall, the assessments take into consideration the five regulatory requirements[17] put forward in the AI white paper. To be more specific, the cost is based on centrally identified activities involved to comply with each requirement.

The estimated compliance cost of an AI unit revolves around the five mentioned requirements, and is projected by several experts and industry stakeholders as follows: (Assuming 170.000 EUR in development costs[18]) This includes i) Training Data: 2.763 EUR; ii) Documentation and Record Keeping: 4.390 EUR; iii) Information Provision: 3.627 EUR; iv) Human Oversight: 7.764 EUR and v) Robustness and Accuracy: 10.733 EUR. Therefore, an estimate of the annual labor compliance cost for one AI model is projected to be 29.277 EUR. To put this in perspective, when extrapolated to the global AI industry it is estimated to range from 1.6 - 3.3 BEUR in total compliance cost, with the assumption that 10% of the AI units are defined as high risk, and therefore are subject to regulation[19].

ANNUAL LABOR COMPLIANCE COSTS FOR ONE AI MODEL



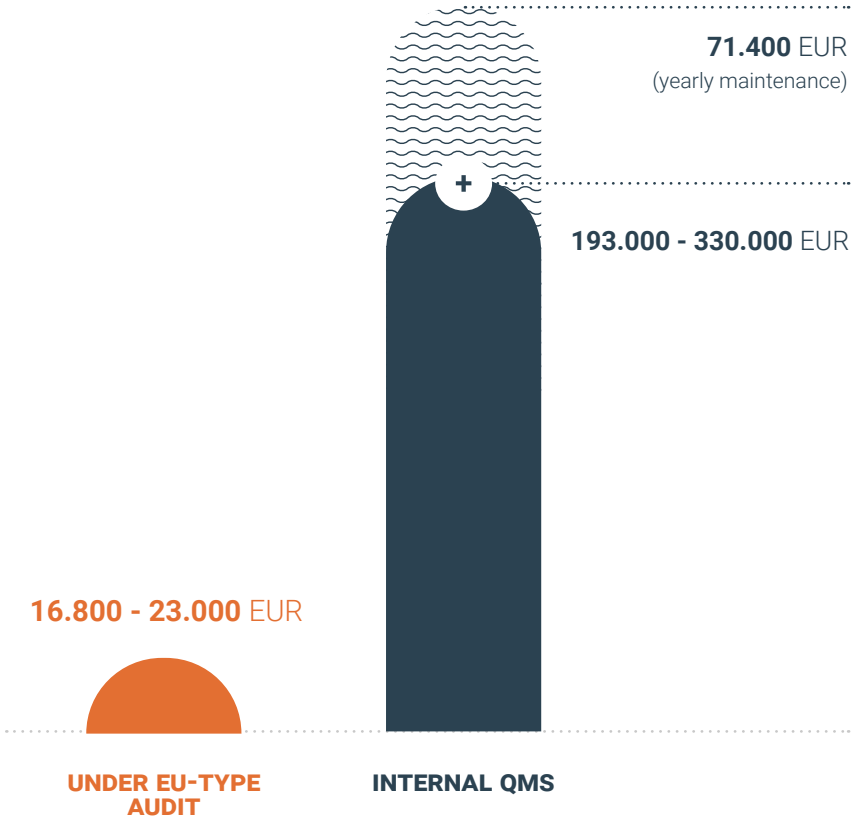
16/17 European Union (2021). *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe* https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195 P. 11

18/19 *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe* P. 11-12

Besides the annual labor compliance cost for a single AI product, the second part of the cost assessment concerns the cost of acquiring a certification process of an AI model through a conformity assessment. Two different estimates of achieving this are put forward: Estimated cost of an ex-ante conformity assessment under an EU-type audit or an estimated cost of an ex-ante conformity report done by an internal QMS. It is estimated that affixing certification on an AI unit, through the EU-type auditing, would range between 16.800-23.000 EUR (10-14% of development costs)[20]. In comparison, setting up an internal QMS can cost between 193.000-330.000 EUR with 71.400 in yearly maintenance costs[21]. However, it is important to take into consideration that most of these costs from building a QMS can, on a larger scale, be split among multiple AI units. Furthermore, there is also the possibility of multiple organizations joining forces and building a QMS together. Although in terms of alignment, planning, and business expenses this could be very costly and time-consuming.

20/21 *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe* P. 11-12

ACQUIRING CERTIFICATION COSTS



Conclusively, when adding it all together the governance related costs include annual compliance costs of 29.277 EUR per AI model and a cost for the certification process where two options exist. Either through an internal QMS or an EU-type examination where the costs of the latter costs would amount to 23.000 EUR. This would leave us at an estimated total cost of 52.227 EUR per model per year. From our perspective these costs are relatively conservative since they only look at one of the calculations relative to the model development expenses. They however, do not take into account the costs related to retraining of the model which could make a model with high-frequency retraining more costly then a rather static model. In total the suggested costs calculation are, however, a good indication and with adding an extra cost of lety say 1-4% of the development costs per retraining and or change request, then one would get a pretty complete picture.

TOTAL GOVERNANCE RELATED COSTS PER YEAR

It is without a doubt a tentative estimation based on knowledge from experts and stakeholders in the market. The final content of the regulation, the number of AI products being listed as high risk, and how much business will rely on pre-trained AI systems or develop in-house are all unclear factors that need to be weighed. However, it is certain that you as an organization need to be prepared for what will be the new norm. At this point one has also to be aware of the limits that these estimates have. They are for example not taking into account which costs arise during the lifecycle of the model incl re-certification etc. and with this only show the initial setup to reach compliance.

SECTION 4

Actions to Take

It is important that organizations that develop or utilize AI consider the strength of their existing governance mechanisms. AI is becoming an increasingly important topic of interest to regulators, not only in the EU but also across many other major economies, including the U.S. and the U.K. One needs to consider whether you currently apply appropriate steps to manage the risks related to AI systems. You need to ensure that adequate controls are in place to comply with existing regulations, including privacy, consumer, and anti-discrimination legislation.

In the following sections, we outline proposed action points to be taken based on the EU Artificial Intelligence Act. We will start each part with the motivation of the Act and then raise some practical problems related to this particular challenge, and then propose how to best address the challenge presenting a practical approach to ensure proper handling of the specific requirements.

4.1. Code of conduct

Title IX of the law deals with the code of conduct. ***"Those codes may also include voluntary commitments related, for example, to environmental sustainability, accessibility for persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of development teams."*** The code of conduct then proposes to include the possibility for 'voluntary commitments'[22].

22 Moltzau, A. (2021, April). *The EU Artificial Intelligence Act: The European Commission Proposes New AI Regulations April 21st 2021.* https://medium.com/digital-diplomacy/the-eu-artificial-intelligence-act-db690428f9e7

For organizations that are not familiar with setting up internal codes of conduct, there's a first learning and experience journey to be made. For organizations familiar with setting up internal codes of conduct, this will be an easier journey. However, as most (probably none) of the existing codes of conduct cover the area of non-linear modelings or, in general, intelligent computer systems. Such existing frameworks will lack the specifics that are needed to address the Act. External expertise is needed, while potentially upgrading internal capabilities.

> ***Actions to take:*** *Equally important like the code of conduct, is the system that supports its enforcement. One solution is the traditional 'tick the box' approach, but more 'digital proof' solutions should be considered, as these will deliver higher reassurance that the conduct actually is followed, which lowers the risk of non compliance with the Act. The more automation can be established in the monitoring, tracking verification and certification process the better.*

4.2. Following requirements

The EU regulation splits the requirements into Title I to XII[23]. Across these titles, the law states the different requirements for high-risk models[24]. It also proposes ways to govern them. The AI regulation lists these points that need to be fulfilled:

1. Using high-quality training, validation, and testing data
2. Using documentation and design logging feature that ensure continuous documentation
3. Ensuring transparency and informing the user about the application of AI systems
4. Ensuring human oversight throughout the process
5. Ensuring accuracy, robustness, and cybersecurity of the system

With more regulation, it will become increasingly difficult to keep track of everything. This has already been the case in established industries such as finance. If the systems are dynamic one might have a problem using established approaches. It is important that you can track changes and automatically test whether or not the AI system is still compliant. It has been shown that many companies have, for example, predicted credit scores using old models, which are no longer up to date and accurate. If the models are then retrained without doing all tests required they might end up with a better model but with some gender bias. So first it is important to know what are the requirements then knowing that something is wrong and last to enforce changes.

23 Moltzau, A. (2021, April). *The EU Artificial Intelligence Act: The European Commission Proposes New AI Regulations April 21st 2021.* https://medium.com/digital-diplomacy/the-eu-artificial-intelligence-act-db690428f9e7

24 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

Actions to take: *An appropriate solution to fullfill the requirements from Title I to XII must be a minimum ability to automatically track and document for critical technical elements of your model implementation for all the five areas mentioned. Be careful to select a solution, which not only handles the current requirements, but are robust, flexible and not leave you with too many manual processes. The more automation, the more digital 'proof,' the better.*

4.3. Data ethics

Data governance forms an integral part of the obligations that are intended to apply to providers of high-risk AI systems. The regulation requires providers to employ a range of techniques to datasets that are used in the training, validation, and testing of machine learning and similar technologies. This includes identifying potential biases, checking for inaccuracies, and assessing the suitability of the data. The act of the EU Commission stresses that you should have data privacy and no bias in the data[25]. The requirements of the General Data Protection Regulations (GDPR) have to be fulfilled[26] and the Artificial Intelligence Act builds on the GDPR requirements. The act furthermore outlines that the used datasets have to be of high quality and fulfill the set requirements for no bias or missing information[27]. The quality of the data sets is emphasized in multiple areas of the act[28 29] and is relevant throughout. Furthermore, most of the work of data scientists is focused on working with the data. Having no bias in it is a core requirement to not end up with a biased model that makes wrong suggestions.

The data foundation is critical to the way a model works and it is important to also examine the data used and output to ensure that a model is performing as expected. It is important to understand what variables may be impacting the outcomes of a model including examining which variables carry the most weight in outcomes compared to expected results. The data being used might be poorly sampled or biased. It is also important to be mindful of other issues related to privacy and general data protection[30].

Actions to take: *The data scientist needs supporting tooling allowing to detect data bias (and more). Only the right tool set will ensure that the model has at all points in time no ethical issues.*

25 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.*

26 *The EU Artificial Intelligence Act: The European Commission Proposes New AI Regulations April 21st 2021.* https://medium.com/digital-diplomacy/the-eu-artificial-intelligence-act-db-690428f9e7

27/28 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

29 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* P.82

30 Preuß,B. (2021), *Contemporary Approaches for AI Governance in Financial Institutions Working paper contemporary approaches to AI governance. SSRN, 1-12* , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773581

4.4. Automatic documentation

You need to have documentation of your models, your code, and the system your models are running in. It is essential that you can document what is happening with the model and track who has made changes or updates. Because machine learning is changing the model through the learning cycle every time it retrains, it requires automated documentation. Manual documentation would be quickly outdated and with this insufficient. The EU describes in their document[31] "CE marking as an indication that a product complies with the requirements of a relevant Union legislation regulating the product in question". To fulfill the requirements of such documentation, the system in which a model runs needs to be able to automatically generate the necessary documentation. The commission further set a quest for a continuous evaluation of the compliance of AI systems with the Regulation[32].

Documentation is the main challenge in the process. A manual documentation is not possible to do without increasing the overhead costs significantly. Another problem that emerges is that in automated retraining scenarios, the model needs to report performance metrics automatically to a log. This can not be done manually, because the retraining process is also not manual and may not involve any human interaction.

> ***Actions to take:*** *You should consider a solution which offers multiple ways to log information. from the model, the ingested data, and the system in general. Please note that the whole process also needs to work with fully automated retraining scenarios. And still needs to be transparent.*

31 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

32 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

4.5. AI platform with immutable logs

The recently suggested framework describes logging obligations to enable users to monitor the operation of the high-risk AI system[33]. This logging has to be designed in a way so they document the reality and hence this has an immutable nature. After-log changes are not possible and all actions performed with the data, the model, or system can be seen. This limits the risk of hidden actions or manipulations. One requirement stated in Title III chapter 2 of the AI Act [34 35] is the ability to evaluate continuous compliance of AI systems with the Regulation. This requirement can only be fulfilled if a logging system is in place that can not be changed afterward.

Central problems that can emerge include that the logging in place could be changed over time or even be removed. This will violate the quest for immutable documentation and would make section 4.4 of this document not fulfilled. Only non-changeable logs can live up to the requirement of documenting issues that have happened. This is by no means means that someone cannot solve the technical issues, but it should be possible to see what happened over time, including that a certain system has not fulfilled the requirements at one point in time.

33/34 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

35 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.*

Actions to take: *You should consider a central datastore, a system that captures both technical information from the environment, models, and data as well as other provided information through assessments that are run by professionals working on a problem. The captured information must be stored in an immutable database.*

4.6. Make automated rules

In the requirements of the European Commission, rules play a central role[36]. These go from general data protection rules like stated in the GDPR and go further to specific model-related roles. In the EU Artificial Intelligence Act, regulators mention the quest for harmonized rules that should apply across the Union to ensure a stable legal base. In the request for quality data, the proposal completes the frame set by GDPR[37]. To ensure data quality, the framework raises the need for continuous testing of the data and the data model interaction. This can be interpreted as the influence of certain biases in the data on the model prediction. The quest for testing the regulation raises the need for a system that supports the organization in doing this. Building on top of the sufficient logging functionality, one has to be able to quickly check the compliance with the various set out rules for data protection, bias, model performance, etc. In Title V the act suggests a supportive system that in the end can also support the innovation without risk of violating the act[38].

General problems emerge not only from the points stated in the act but also generally from the focus areas of different personnel. We can say that the points raised in 4.4 and 4.5 build the foundation for the required documentation. However, in practice one can say that the interpretation of such logs might only be given to technical persons. Without sufficient technical knowledge, it might be difficult to see whether a model, data set, or system of models complies with the regulation. The act states multiple rules and tests that should be performed. Performing these tests will increase the manual work burden that data science teams face when building models. These problems lead to the quest for a way to translate the technical logging into human-understandable rules and checks that can be understood quickly from less technical personas. Ideally, these rules can serve in addition to the fundamental logs as documentation to auditors.

Actions to take: *To reach taceable compliance you have to consider a flexible rule engine that can interact with the data stored. A key feature will be a detailed visualization of the data in dashboards, a compliance manager can get a quick overview whether a certain set of requirements (either internal or external) is fulfilled or not. Automated compliance checks can become a part of the evaluation of conformity assessments or other evaluation steps.*

36 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

37/38 *The EU Artificial Intelligence Act: The European Commission Proposes New AI Regulations April 21st 2021.* https://medium.com/digital-diplomacy/the-eu-artificial-intelligence-act-db690428f9e7

4.7. Make your own certificates

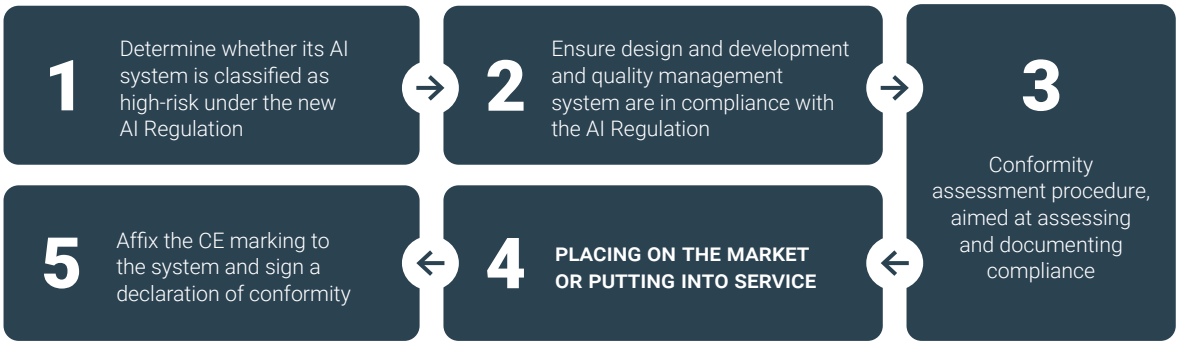
As stated in the act[39 49 41], the suggested act is only the European-wide suggestion. This means that national authorities or industry-specific regulators might publish one interpretation or amendments to the act. The act also opens for organization-specific adjustments and additional checkpoints. While the GDPR's introduction of the principle of accountability was a significant step-change in privacy law requiring organizations to put in place practical measures to demonstrate compliance, the AI regulation is even more ambitious. Providers of high-risk AI systems are expected to implement comprehensive governance and risk management controls.

This includes the need to create a strategy for regulatory compliance, procedures, and techniques for the design and development of the AI system, and a process for evaluating and mitigating the risks that may arise throughout its entire lifecycle. Conformity assessments will also need to be undertaken to demonstrate adherence to the regulation's requirements.

39 *The EU Artificial Intelligence Act: The European Commission Proposes New AI Regulations April 21st 2021.* https://medium.com/digital-diplomacy/the-eu-artificial-intelligence-act-db-690428f9e7

40 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

41 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.*



The EU Artificial Intelligence Act is a great fundamental framework touching on the most important areas that need to be watched. However, one might see organizational, national, or regional specific requirements. That means that the option to adjust assessments or to make one's own assessment should be given. Specific organizational adjustments could be extra questions or additional metrics that one wants to log for a given AI system. The system has to be as flexible as possible to accommodate all the requirements that might come up. And this both today but potentially also for the future. This is as much a practical request as one related to sustainability.

Actions to take: *Changing regulation and the need to fit the suggestion to ones organization raise the need for a felxible system which can incorporate legal but also compliance requirements set by the organization itself.*

4.8. Allow teams to experiment in a sandbox environment

In Title V the act talks about regulatory sandboxes in Art. 53 and 54[42] [43] . In sandboxes, one should be able to test settings and the models as well as the interaction with any data used. The experiments, however, have to lead at one point to solutions that fulfill the requirements of the act. Meaning that the to-be-tested requirements are not just functional or statistical but also regulatory in nature. This requires that already at this stage all the possibilities to fulfill the requirements need to be given (including Assessments, logging, etc.). The act describes it in Title V like this: "AI regulatory sandboxes establish a controlled environment to test innovative technologies for a limited time on the basis of a testing plan agreed with the competent authorities."[44]. It, however, also states that "...AI regulatory sandboxes and other measures to reduce the regulatory burden and to support Small and Medium-Sized Enterprises ('SMEs')..." [45] [46] This shows that the commission is aware of a certain burden that the regulation can bring to the development of models and systems.

The general problem today is two-sided. On one side we see that models are often developed in a sandbox environment or in a POC type environment, where no regulatory consideration or requirements are included. Wanting to move these models into real-live production will often mean that much if not alle the model development will have to be redone with regulation and the required documentation in place.

> ***Actions to take:*** *From the start of a project you need a clear understanding of the regulatory compliance that might be required for taking your model into production. This needs to be combined with an achievable plan on how to fulfill regulatory requirements now and in production.Without sufficient logging and reporting functionality it might be difficulut if not impossible to comply with the regulatory requirements.*

42 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

43/44 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.*

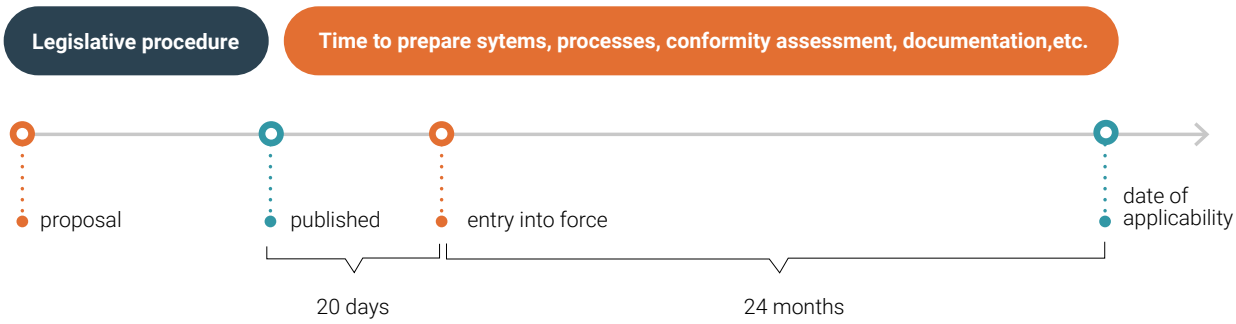
45 *A European Strategy for Artificial Intelligence* [PowerPoint slides]. Digital Industry DG CNECT, European Commission.

46 *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.*

THE EU'S AI ACT

What Will Happen Next

This is the beginning of a debate on how AI should be regulated in the future. The next step that will shortly follow is for the proposal to be reviewed and debated by the European Council and Parliament. Once adopted, the regulation will come into force 20 days after its publication in the EUR-Lex Official Journal of the European Union. It will apply 24 months after that date, but some provisions from the regulation will apply sooner. From that date, it can be fully invoked by its addresses and will be fully enforceable.



You should start addressing the act as soon as possible. Why should you not wait until it is finally decided? The transition to the GDPR requirements was not always smooth in organizations around Europe and this AI-related regulation is more complex, has more touchpoints to the organization, and the proposed fines are also much higher.

Implementing AI systems the right way from the beginning and thinking about **scalability, integration as well as compliance from day one, will both ensure legal compliance as well as cost savings.** In detail it means that code does not need to be rewritten and models can be replicated across different entities. Similar structures ensure furthermore that the maintenance burden is reduced and so costs. It is also a headstart in terms of the competition that might need to spend a lot of money and time to bring their experimental settings to be ready for production and scale. If one follows a production ready approach from day one, this results not only in faster time to implementation but also allows stakeholders to keep a vision of the end system in mind. A setup like this will ensure that projects do not die out due to missing interests or too complicated and long implementation projects.

Please stay tuned for the next whitepaper from 2021.AI in July 2021, which will focus more on the models which will fall in the High Risk Model definition and other type of high risk disruptive technologies.

> *Scalability, integration as well as compliance from day one, will ensure legal compliance as well as cost savings and an easy transition from PoC stage, to beta stage and further on to production.*

Contact Details

- **Björn Preuß** (Senior Lead Data Scientist 2021.AI) bpr@2021.ai

2021.AI

GET STARTED

2021.AI serves the growing need for enterprise-wide AI. Our Grace Enterprise AI Platform seamlessly orchestrates AI across all levels of an organization while offering comprehensive AI governance solution to help clients reach regulatory excellence. 2021.AI is headquartered in Copenhagen with sales and R&D in several locations.

Ryesgade 3F, 2200, Copenhagen N, Denmark | CVR. 3783 6303 | + 45 42 67 04 97 Copyright 2018 - 2021.AI all rights reserved.