Luxoft
A DXC Technology Company

The new Artificial Intelligence Act and its repercussions for automakers

by **Wojciech Domski**, Senior Solution Architect

The EU AI Act — be smart, act now

Artificial Intelligence (AI) is increasingly present in our lives. The European Union (EU) is trying to regulate the use of AI with the 'Artificial Intelligence Act'. This regulation is still a proposal, but it will have a tremendous influence on the software industry when it comes into effect. In this article, we look at the details of the act, what consequences it could have on people, and what actions we can take now. It's time to prepare for changes.

AI in our everyday lives

AI is everywhere. When you search for a film on your favorite video-on-demand app, the app uses AI to recommend titles based on your viewing preferences.

When shopping online, AI-based software presents you with products that you should buy, based on your previous orders. Even while this article is being written, the word processor shows hints about vocabulary, grammar or even suggests how to end a sentence.

AI at work in our everyday lives

AI in the car

AI and autonomous driving

AI is also present in cars. Here, it assists the person behind the wheel with features such as automatic collision avoidance, but it also works in the background: AI analyzes huge amounts of data coming from various sensors in the car. Rule-based conventional algorithms wouldn't be able to process these huge amounts of data in real time. They also couldn't handle all potentially unforeseen real-world cases efficiently. With fast growing efforts in autonomous driving (AD), it has become clear that AI-based systems will play an indispensable role within the AD domain.

The immense use of AI has caught the attention of the European Commission. In 2021, the European Parliament and the Council proposed a unified approach in the regulation of AI-based systems.

Regulation details

The document introduces scope and definitions of AI systems, creating a common baseline of what they are and how they should be developed and maintained.

Three domains

According to the proposal, the new regulations — if accepted — should apply in **three different domains:**

1. **Providers of AI systems**, irrespective of whether they reside inside or outside the EU
2. **Users of AI systems** who are located within the borders of the EU
3. **Providers and users** that are located outside of the EU, but the output of an AI system is used within the EU

Note that in the third domain, the providers and users are considered together, making it the most important and complex domain. The regulations will apply to all cases where the AI system or its outputs can have any impact on EU citizens.

What counts as an AI system?

The regulation defines an AI system as a software that was created using at least one of the following approaches:

Machine-learning approaches

Logic- or knowledge-based approaches

Statistical approaches, including search and optimization methods

This definition establishes a broad spectrum where multiple solutions, which were previously not seen as AI-based, now might be considered AI-based.

Risk types

The proposal defines three types of risk when using AI. These are derived from a risk-based analysis. The **three risk classification types** are:

Unacceptable risk

High risk

Low or minimal risk

Let's look at each of the risk classes individually.

Unacceptable risk

The unacceptable risk group includes solutions that immensely interfere with a person's life. AI of this kind is strictly prohibited. For example, the use of AI to exploit any vulnerabilities of a target group — like the age of a person — is not allowed, as this could cause physical or psychological harm. A system that estimates the trustworthiness of a person is also banned.

Additionally, the use of remote biometric identification in public space is also prohibited in principle, but there are exceptions: Under some restrictions remote biometric identification may be used to "achieve a substantial public interest" [1] (e.g., for a targeted search of crime victims like missing children[2]).

High risk

High-risk AI systems feature different ways of monitoring. A high-risk system is a safety component of a product or a product in itself. This means a system that is aided by AI can also be considered as a high risk. As such, it would need to undergo a third-party conformity assessment to analyze and determine if it fulfils the directives and regulations of the EU. During the assessment, different criteria are considered: The intended purpose of the AI system must be analyzed, as must its potential to cause harmful effects on groups of people. If a dataset is used to train a high-risk system, then additional regulations apply.

Low or minimal risk

The low risk group is a category for systems that don't fall into any of the previously mentioned groups. However, that doesn't mean that additional actions should be neglected. This class of systems doesn't require a strict policy to track the life cycle of an AI-based system. Nevertheless, providers of low risk or embedded AI systems are still encouraged to disclose a code of conduct and technical documentation.

A procedure to assess conformity with EU regulations has already been defined (see references [CapAI]). The document provides key points on how to assess the risk group affiliation of a system and describes measures that system providers ought to take.

1. See references [Regulation], Introduction (19) and Article 5.1 (d).

2. In this context, also concepts for a European amber alert need to be reviewed and eventually rebuilt.

Dataset groups and analysis

The AI Act states that the dataset should be divided into three groups: Training, validation and testing. This is a common and well-adopted practice for supervised learning.

The EU proposition also covers other aspects of dataset preparation. It stipulates:

- An analysis of the dataset and its potential to introduce biases
- The documentation of the preparation process
- A reflection of the current state of the system in the technical documentation

More aspects to consider

The proposal concentrates on defining AI, but it also contains regulations for aspects that only indirectly belong to the AI domain. Let's look at some of them in detail.

Logging creates additional costs

An aspect that is close to automotive and aerospace, is record keeping. Through the regulations, the system should be able to log all events and interactions to an extent that allows further analysis of the data. This aspect puts additional costs on vendors:

Storage costs

If data storage systems were to be used in a car, data should either be stored locally or transferred via an internet connection to a remote storage location. Both solutions require added investments to operate in accordance with the proposed regulations.

Operating costs

A direct cost can also be associated with human oversight. An AI-based system must be developed to offer tools that allow manual monitoring. This creates at least two potential cost sources: A direct one related to an employee who needs to be involved in the process, and a second one related to the tools themselves.

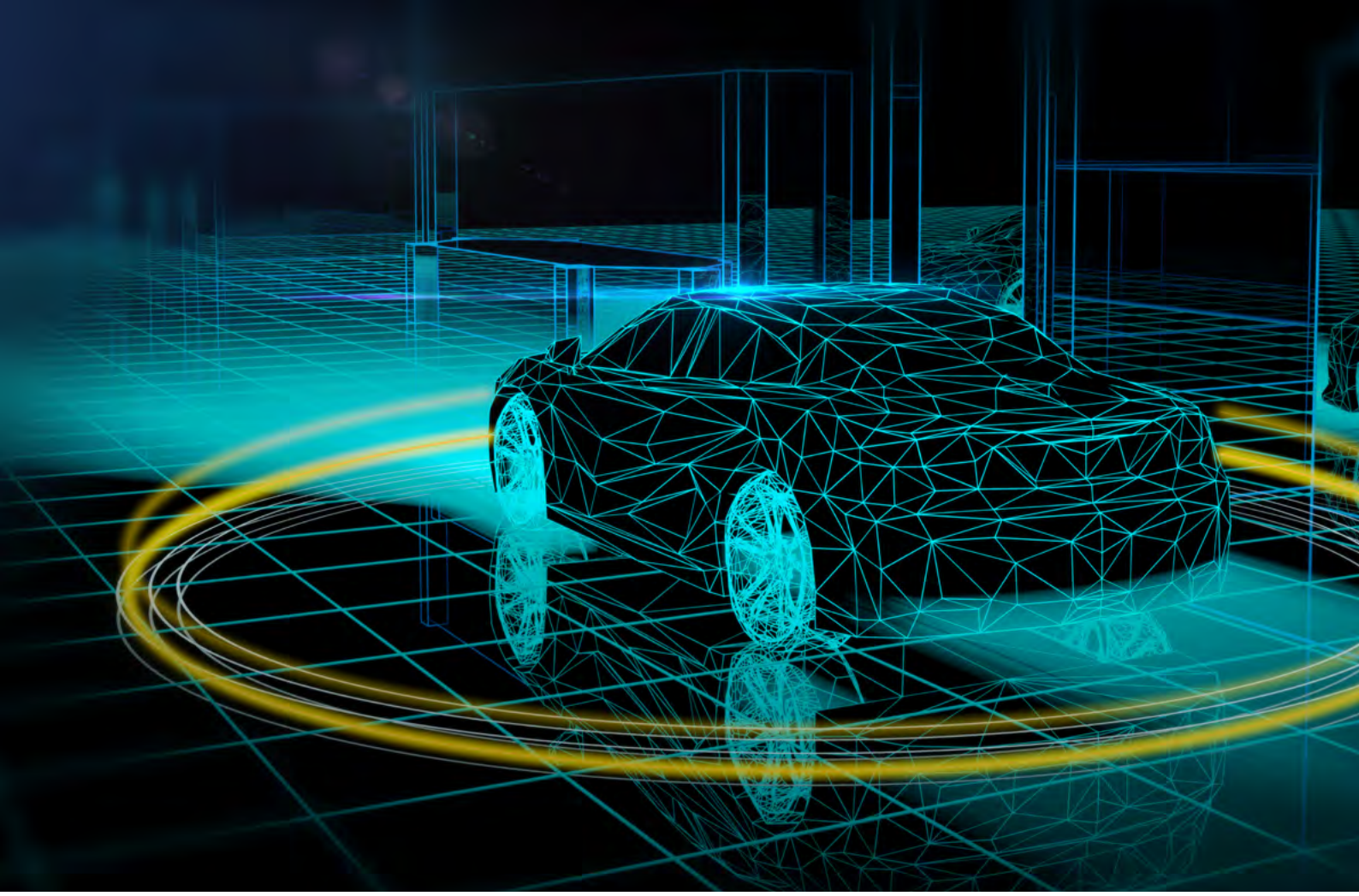
Development costs

Usually, the tools that help with the analysis are created and used by developers. If the tools currently used can be adapted, this is the way to go. But if tool adaptation isn't possible, then a new toolchain is required — creating even more costs.

Planning and implementing logging and data storage in advance can help reduce the risks of unsuspected costs later.

Handling and allowing access to data also adds to the costs, as it can be more complicated than expected. Automakers and their suppliers interact in various networks and partnerships, sharing and accessing data in numerous ways: This has to be handled and controlled. For example, data may be fragmented to reflect different car generations or partnerships. Data may be split into subgroups to restrict access for certain partners or participants may want to add data (which can mean transferring hundreds of Petabytes for AD).

With the EU AI Act introducing even more restrictions and limitations, data-driven AI development costs are likely to rise. If, for example, an AD system is generated and trained outside the EU, but used inside the EU, the system needs to comply with the EU AI Act.



Security

With the number of security incidents constantly growing, it's crucial to provide an additional layer of protection to the systems. This aspect is also covered in the EU proposal: Although it doesn't clearly define or provide guidelines on how to enforce a security policy on AI-based systems, it creates awareness of the security aspect of AI.

This also has the potential to increase the general understanding of how an AI system works. By pointing out influencing factors in a more transparent way — therefore minimizing security concerns — decisions in the area of AI systems are easier to make. This direction of research and development is also referred to as explainable AI (XAI). Its goal is to build trust in an AI system, mainly via increasing transparency and understandability.

The risk assessment phase in particular will benefit decision makers, developers and users of such systems, but also security-focused approvers (e.g., during vehicle homologation).

Security — as functional safety in general — is crucial for the proper operation of any system. Let's focus on a vision system that should automatically recognize signs to provide drivers with some meaningful feedback. A good example is an intelligent speed assistance (ISA) system, which we discussed in an **earlier post**.

Because the system is highly dependent on the input data, it's possible that feeding the system with a forged input could lead to incorrect sign recognition. With AI-aided vision systems, this type of attack is called an 'adversarial attack'. What's more, it doesn't require a direct interaction with the system. A specifically designed sticker, which is then put on a traffic sign, could prevent the system from recognizing the sign, and could alter the outcome of the classifier-system.

We will discuss the challenges of sign recognition in more detail later in this series. Stay tuned.

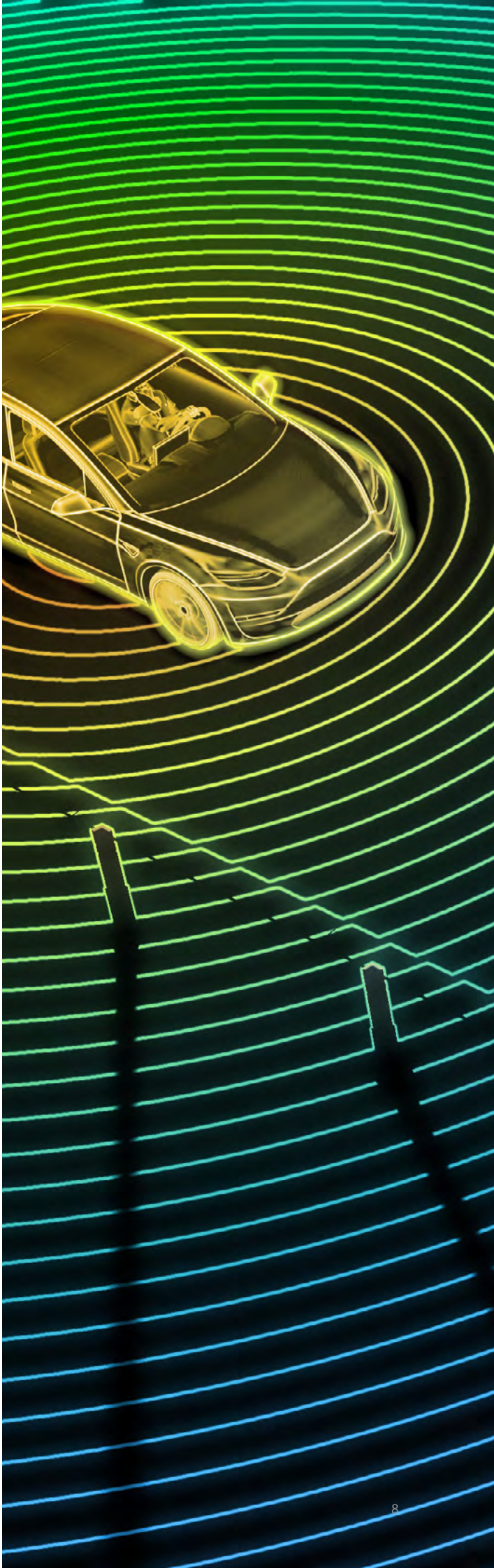
Act now to be prepared

The proposal of AI regulations has a potent influence on the AI systems. These systems are gaining popularity — thanks to their ability for adaptation and versatility. The multiple restrictions and limitations enforced on such systems help society, so that its people can thrive and feel safe.

However, a number of requirements will increase the costs of developing and maintaining AI systems, presenting new challenges for businesses. It's time to adapt to the upcoming changes: Act now to be prepared for the future of AI.

Get in touch

At Luxoft, we offer a variety of AI expertise. If you need advice or want to ensure that you're compliant with the AI Act, get in touch:
luxoft.com/contact-form



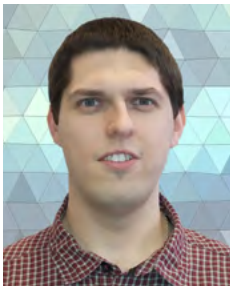
References

[TheAIAct] The Artificial Intelligence Act.

[Regulation] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS.

[CapAI] L. Floridi, M. Holweg, M. Taddeo, J. A. Silva, J. Mökander, Y. Wen, capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act, 2022.

About **the author**



Wojciech Domski
Senior Solution Architect

In 2019, Wojciech obtained his PhD degree in Robotics. His main area of expertise is mobile robotics, including modeling, path and trajectory planning and motion control. Besides robotics, he specializes in embedded systems and AI-based systems. Since 2020 he has worked at Luxoft, where he participates in projects aimed at delivering solutions for autonomous vehicles of SAE Level 3 and higher.

About Luxoft

Luxoft is the design, data and development arm of DXC Technology, providing bespoke, end-to-end technology solutions for mission-critical systems, products and services. We help create data-fueled organizations, solving complex operational, technological and strategic challenges. Our passion is building resilient businesses, while generating new business channels and revenue streams, exceptional user experiences and modernized operations at scale.

luxoft.com