

#BSP_ Paper August 2021

Artificial Intelligence Act

Business & Science Poland (BSP) welcomes the possibility to comment on the proposal for a Regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts (COM (2021) 206 final). We represent leading Polish entities particularly from energy-intensive industry, air transport, cyber and IT sector, postal services and financial markets employing over one hundred thousand employees in Poland, other European Union (EU) Member States and outside the EU. BSP is also in a partnership with R&D, academic and SME organizations. Topics related to Artificial Intelligence are within the scope of our interests.

We welcome the intention of making the EU a leader in the development of safe and trustworthy Artificial Intelligence (AI). The new regulations are aimed, on the one hand, at building trust in Artificial Intelligence systems to reduce the associated risk. On the other hand new regulations are focused on supporting investment in Artificial Intelligence and further development of this technology. We would like to focus on several issues identified in the analysis of the proposed regulations.

AI is a rapidly growing group of technologies that can deliver many different socioeconomic benefits across all industries and areas of social activity. Due to the pace of technological changes and in the light of potential challenges, the EU is striving to develop a well-balanced approach. It is in the interest of the European Union to maintain the EU's technological leadership and ensure that Europeans can benefit from new technologies designed and operated by following EU values, fundamental rights, and principles.

We understand that the aim of proposed regulations is to ensure security and respect the fundamental rights and values of the EU. We agree with this and consider actions in this regard as necessary. At the same time, we would like to note that the mechanism proposed in this regulation is not the most optimal and may result in a series of undesirable side effects in the form of freezing the development of AI, as well as shifting AI development centres outside the EU. Therefore, we propose several improvements in this area.

In particular, we would like to highlight the following aspects of the AI regulation:

1/ High-risk AI systems

In the discussed regulation proposal, it is recognized that the application of a risk-based framework is a better solution than the general regulation of all AI systems. Risks and hazards should be determined on a per-sector and case-by-case basis. The risk measures should also give the consideration to the legal and safety implications.

In our opinion, the category of high-risk algorithms is too broad. Deeming all algorithms applied to the critical infrastructure as high-risk (Annex III) will paralyze the development of the domain in the currently least digitized industry, such as energy and petrol sector. Algorithms allowing for internal optimization of raw material consumption, predicting hydrocarbon quality as well as allocation of means of transport for fuel delivery to terminals or stations should not be the subject of these regulations. They are an element of the improvement of operational excellence in enterprises. High-risk algorithms used in the energy and petrol sector do not concern the end customer and do not cause the risk of discrimination on human rights. We therefore strongly recommend that this category be excluded from the definition of "high-risk" algorithms.

2/ Record-keeping of the high-risk algorithms

We would like to lay down another solution than an automatic registration of all high-risk algorithms. In our opinion, the reverse mechanism should be used – i.e. allowing users to request conformity assessment and verification by audit bodies through raised objections if needed. We find that enabling to use only the "certified" algorithms will significantly slow down the development of AI in the EU and at the same time it will cause uncontrolled migration of algorithm development centers outside the EU, in particular to the US and China, and consequently will not solve the problem posed by regulations.

The proposed provisions impose an excessive administrative burden on the suppliers of the algorithms and in consequence it will delay the technological development of many industries, thus cause suboptimal resource management by enterprises.

3/ The requirement to confirm the compatibility of algorithms in each case (conformity assessment)

The proposed requirement to confirm the compliance of the algorithm in case of every substantial update of the algorithm does not bear in mind that the algorithms require, since their fundamental assumptions, regular and systematic updating, "learning" and "tuning" on the basis of real time data. As a result, an indented and targeted purpose that an algorithm could be 'frozen', certified and implemented may never be reached. On the contrary, the algorithms are constantly evolving. As a result, issuing consent only for a specific version of the algorithm, without consideration of its future modifications, will result in the use of an outdated SI algorithm (developed on the basis of historical, not real time data). This may result in duplicating the algorithmic bias as the algorithm would be trained on a limited data pool. With this in mind, we acknowledge that reporting standard deviations would be more effective solution than issuing approvals for release to use.

4/ Penalties for non-compliance with the regulation

In our opinion, the fines for the non-compliance of a high-risk Artificial Intelligence system with requirements under the proposed regulation are too high. Businesses or public authorities that develop or use AI applications that constitute a high risk for the safety or fundamental rights of citizens would have to comply with specific requirements and obligations. Compliance with these requirements would imply costs amounting to approximately EUR 6000 to EUR 7000 for the supply of an average high-risk AI system of around EUR 170000 by 2025. For AI users, there would also be the annual cost for the time spent on ensuring human oversight where this is appropriate, depending on the use case. Those have been estimated at approximately EUR 5000 to EUR 8000 per year. Verification costs could amount to another EUR 3000 to EUR 7500 for suppliers of high-risk AI. Businesses or public authorities that develop or use any AI applications not classified as high risk would only have minimal obligations of information. However, they could choose to join others and together adopt a code of conduct to follow suitable requirements and to ensure that their AI systems

are trustworthy. In such case, costs would be at most as high as for high-risk AI systems, but most probably lower. We recommend considering provisions applying 'warnings for non-compliance with the regulation' and lower level of financial fines than those proposed for a given entity.

5/ High-risk AI system -based places - data storage

We recommend that the servers processing high-risk data, for cybersecurity purposes, should be located only within the European Union.

6/ Conformity assessment for AI systems at the national level

There is a defined line for the exchange of information and good practices among domestic operators to carry out third-party conformity assessments for AI systems intended to be used for the remote biometric identification of persons.

7/ Document retention

Please note that in the event that the company will exist for less than 10 years, the supplier should not keep the data at the disposal of the competent national authorities for 10 years after placing the AI system on the market or for personal use.

8/ Applications using AI

We fully agree that applications using AI and applications that violate the fundamental rights and affect the rights of children, should be banned in the EU. We suggest that the EU requires companies to demonstrate that their claims and assumptions are backed by science, that they do not violate any of the fundamental rights, and do not discriminate against users, before the market launch of their applications or products that use artificial intelligence.

9/ Bayesian techniques

The list of techniques in the Annex I include technologies that are not normally considered to be Artificial Intelligence (e.g. traditional data analysis tools). For example, Bayesian inference is not an Artificial Intelligence, but proven mathematical formula.

10/ The error free data

As we know from working with large data sets, complete error-freeing and completeness of the data obtained are not possible. Data are interpreted by experts, and even in their line of reasoning, errors can creep in. However, this does not mean that the data should not be as accurate as possible. Therefore, the recommendation should be broader or contain various types of labels to distinguish data - from false, artificial, with minor errors, to those closest to the ideal.

About BSP

Business and Science Poland (BSP) connects the experience of leading Polish enterprises with the EU agenda. We represent the knowledge and interests of successful entities, which employ over 100 000 workers in Poland, EU and globally. We are committed to advancing the values of EU Common Market in sync with the needs to transform it responsibly and effectively.