



EUROPE'S
VIDEO GAMES
INDUSTRY

Comments to the European Commission Inception impact Assessment regarding the proposed policy options for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.

10 September 2020

Transparency Register Identification Number: 20586492362-11

Introduction

1. *ISFE welcomes the opportunity to submit comments to the European Commission Inception Impact Assessment regarding the proposed policy options and instruments for Artificial Intelligence. In June, ISFE responded to the Consultation on the White Paper on Artificial Intelligence – A European Approach in which we (i) described the role of the video game industry in the development and use of AI, (ii) outlined the policy areas of particular importance in building an ecosystem of excellence to support the development and uptake of AI across the EU economy, and (iii) expressed our position as regards the proposed regulatory approach as outlined in the White Paper.*
2. *ISFE represents the video games industry in Europe and is based in Brussels, Belgium. Our membership comprises national trade associations in 18 countries across Europe which represent in turn thousands of developers and publishers at national level. ISFE also has as direct members the leading European and international video game companies, many of which have studios with a strong European footprint, that produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and tablets. The video games sector represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. In 2019, Europe's video games industry saw €21 billion in revenues. We have seen a growth rate of 55% over the past 5 years in European key markets ¹. Video games have a proven ability to successfully drive new business models and adapt to digital transformation: online and app-based gaming represents 76% of the industry's total European revenue. Via the emergence of on-demand and streaming services and the launch of new high-performance consoles, together with the strong growth of mobile gaming, the industry offers players across Europe and in all age groups the possibility to enjoy and engage with video*

¹ ISFE Key Facts 2020 from GameTrack Data by Ipsos MORI and commissioned by ISFE <https://www.isfe.eu/isfe-key-facts/>

games². Today 51% of Europe's population plays videogames, which is approximately 250 million people, and 45 % of the players are women.

3. *The video game sector plays an important role in research and development of Artificial intelligence (AI), and AI is used in innovative and creative ways by the industry to create new compelling experiences for players. Also, the simulated worlds of video games constitute a researcher-friendly environment: video games are rich and complex, but controllable environments providing important feedback to the researcher, in particular on which data to collect to further refine research in this area. For further details please consult the ISFE [response](#) to the consultation on the White Paper.*

Comments on the proposed policy options in the Inception Impact Assessment

4. *ISFE welcomes the opportunity to provide its view on the policy options presented in the Inception Impact Assessment. In accordance with our previous contribution to the consultation on the White Paper, ISFE believes that any new legislation must be considered with a cautious approach. New compulsory requirements to low-risk applications would result in a disproportionate diversion of industry resource, stifling innovation, and damaging Europe's competitiveness in global AI development. Because many AI applications pose no, or a low risk to individuals or society, it is important that the approach proposed by the European Commission provides the necessary clarity to ensure that legislation remains proportionate and targeted to fulfil its objectives, to avoid that sectors that do not pose significant risks fall under a specific legislative framework.*
5. *Therefore a legislative act covering all types of AI would not be proportionate and would disregard the legislative framework that is currently in place which apply already today to many existing AI applications. The White Paper recognised that developers and deployers of AI are already subject to European legislation on fundamental rights (e.g. data protection, privacy, non-discrimination), consumer protection, and product safety and liability rules. For example the GDPR already imposes the obligation to inform data subjects of automated decision making and provides them with the right not to be subject to a decision based solely on automated processing if it produces legal effects on them or similarly affects them. The GDPR also places an obligation on organisations to carry out Data Protection Impact Assessments to mitigate any high risks that AI applications may pose before such an AI application is implemented.*
6. *New regulation and/or updating existing legislation in some areas of applications of AI may be necessary, especially where damages may cause substantial harm or pose a material risk of consequential impact on individuals and society, such as facial recognition technology where deployers process and store the data that is collected for example. It is important, however, that any regulatory framework is flexible enough to embrace the evolution of wide AI technology to ensure that Europe remains competitive in strategic areas in the global ecosystem. An important aspect of a high-risk AI regulatory framework would be to clarify which sectors and*

² See also <https://www.isfe.eu/data-key-facts/>

uses should be covered by applicable legislation and which obligations would apply to which actors.

7. Policy option 3 (b) suggests that the EU legislative instrument could be limited to “high-risk” AI applications, which in turn could be identified on the basis of two criteria as set out in the White Paper (sector and specific use/impact on rights or safety) or could be otherwise defined. The White Paper proposed to define a high risk AI application if it is subject to two cumulative criteria: (i) the application is employed in a sector where significant risks can be expected to occur; and (ii) the application is used in such a manner that significant risks are likely to occur. Moreover the White Paper mentions that each obligation should be addressed to the actors who are best placed to address any potential risks. Such clarification regarding which obligations or requirements should apply to developers and which should apply to deployers is important as it is important to recognise the separation, and unique responsibilities, of such roles.
8. A trustworthy and responsible AI approach is important also for no or low risk AI applications. The video game sector promotes responsible data management and takes great care to protect player data – whether used traditionally or by AI - and makes sure the data is used in a manner consistent with privacy principles and regulations, such as the GDPR and the ePrivacy Directive. Many video games companies have adopted or are in the process of adopting their own internal policies or best practices around using AI to address any bias and transparency issues. When decisions are made by AI that affects a player or needs to be further explained, a human-supervised approach may often be used, but not all no or low risk AI application may require this. Video game companies are taking these ethical challenges seriously by developing internal policies on these issues.
9. The Inception Impact Assessment and the White Paper suggest a voluntary labelling system for AI systems that are not considered high-risk. Such a voluntary scheme, as proposed in policy option 2, and further outlined in the White Paper, would be legally binding for those operators that join such a scheme, and in return they would use the AI trust label for their AI application. This may negatively impact AI applications that would not join the voluntary labelling scheme simply because these may apply industry best practices and voluntary frameworks already in place³. A guiding principle for the European Commission should instead be to support organisations that are developing or deploying AI to allow them to identify risks or harms and to ensure guidance on process to follow to mitigate any risks.
10. Flexibility and recognition of best practices should be a focal area of the Commission, to avoid channelling all low risk AI applications into a voluntary legally binding scheme, which could create significant administrative burdens as well as disincentivising investment and innovation

³ For example, Digital Innovation Hubs, such as the Digital Catapult have developed useful guidance for start-ups which support them in their use of, and approach to an ethical AI. Also, the UK regulator the Information Commissioner’s Office (ICO) in partnership with the Alan Turing Institute have very recently issued guidance to give organisations practical advice to help explain the processes, services and decisions delivered or assisted by AI to the individuals effected by them. Most recently, in July 2020 the Independent High-Level Expert Group on AI set up by the EU Commission has published “The Assessment List for Trustworthy AI (ALTAI)” which provides an initial approach for the evaluation of Trustworthy AI and the ICO has published its “Guidance on AI and Data Protection”.

in AI. Guidelines or best practices that are not part of such a voluntary scheme could be as efficient in creating responsible and trustworthy AI. This is especially important to consider because low risk AI must already comply with EU legislation in the field of fundamental rights (e.g. data protection, privacy, non-discrimination), consumer protection legislation, and product safety legislation.

- 11. ISFE believes that for low risk AI such an approach, i.e. policy option 1, should be further supported instead of a 'regulation first' approach. As technology is evolving at a rapid pace, a European AI framework needs to be flexible enough to ensure that Europe remains competitive in strategic areas in the global ecosystem. Competition, technology, and customers are the natural drivers of the market. Steps that would artificially channel developments along a particular path needs to be envisaged with caution.*
- 12. From the perspective of video games where AI applications appear in a controlled virtual environment, while some requirements can be useful guidance because of how AI is used (e.g. to improve the player experience, to ensure that the gameplay environment is safe both from a network security perspective and from a player safety perspective) such as:*
 - a. information and transparency on the purpose and the nature of automated decision making such as AI systems are important to create trust with the player, and where information requirements are foreseen in the GDPR,*
 - b. robustness and accuracy of AI systems are also important, and*
 - c. human oversight in relation to any online interactions such as in the moderation of online communities to support player safety,*

such requirements can be part of guidelines or best practices but do not necessarily need to be part of a binding scheme to be efficient. More generally, given the nature of the proposed low risk voluntary labelling system, which would become binding once a developer or deployer opted in, it would appear disproportionate and harmful to innovation and Europe's competitiveness to require compliance with all the requirements that are required in high risk applications. This would effectively categorise low risk applications as 'high-risk' once a developer or deployer opted in. Furthermore, different requirements are more relevant to different sectors and ISFE would respectfully suggest that the low risk approach should consider the nuances of different sectors.

- 13. As regards enforcement, a careful approach should be taken for low risk AI applications. As stated in the White Paper, the existing EU legislative framework already applies to AI, in particular in the area of fundamental rights. The existing legislation includes enforcement mechanisms specifically targeted to any breaches, whether that is consumer protection legislation or data protection or privacy legislation. Therefore, for low risk AI, the existing enforcement framework is sufficient.*

END

Contact:

Ann Becker | Head of Policy & Public Affairs | ann.becker@isfe.eu