Schibsted

June 2021

Proposal for a Regulation laying down harmonised rules on artificial intelligence

Position paper

Key messages

Schibsted is a family of digital consumer brands based in the Nordics with world-class Scandinavian media houses, leading classifieds marketplaces and tech start-ups in the field of personal finance and collaborative economies. Schibsted constitutes an ecosystem of various brands that offer different products and services to users and customers, and where we utilize data across the ecosystem both to attract users and customers, develop and personalise our products and services, as well as keep users and customers engaged.

Rooted in democratic values, Schibsted has a long heritage of contributing to society. Millions of people interact with Schibsted brands every day to become empowered in their daily lives, e.g. through reading our newspapers, purchasing second hand goods on our marketplaces or utilising our financial services. Schibsted has developed its values through 180 years of free and independent media, founded on a strong awareness of the social responsibility that characterizes publishers' activities. A key guarantor for upholding these values is the principal owner, Tinius Trust, which is also making sure that the values are brought forward into a complex digital world.

Schibsted welcomes the Commission's ambitions for human-centric AI and supports the proposal for a risk-based approach. However, the proposal leaves many questions open about the practical implications for European AI innovation and competitive position.

At Schibsted we are committed to responsible AI innovation to better serve our users and our societies, and to build financially sustainable digital media operations in an increasingly global digital market. However, for our ambitions to become reality, we need clarifications on several issues of the rather vague proposal by the Commission.

- Definitions of prohibited AI must be clarified with clear examples anchored in practice and diverse industrial fields, including journalism.

- Definitions of high-risk AI must be clarified with clear examples anchored in practice and diverse industrial fields, including journalism.

- Further clarity is needed in regards to the obligations and liabilities related to transparency.

- These clarifications, in conjunction with efforts to incentivise compliance, will be central to enabling a level playing field and the furthering of the Commission's and Schibsted's

shared ambitions for trustworthy AI.

Key areas in need of clarification

Prohibited AI

We agree with the Commission's proposal for banned AI application areas, but call for a number of clarifications. Notably, we consider how categories which would be applicable to private companies leave a lot of room for interpretation. This includes formulations such as '*beyond a person's consciousness'*, '*materially distort*' and '*physical or psychological harm*'. We consider the broad definitions to cause disproportionate legal uncertainty for companies utilising AI solutions. It is also unclear whether the harm must be caused directly by the AI solution or would prohibition be applicable to indirectly causing the harm to individuals. For example, displaying certain advertising to a group of individuals is unlikely to cause direct physical or psychological harm to the individuals but it is possible that a particular ad could cause the individual to make a bad decision, which could cause indirect harm to that individual.

In addition, we think that *'manipulative'* and *'exploitative'* AI and its applications must be clarified during the legislative process. As currently understood the threshold for qualification is high, but without clarification the regulation may prove hard to navigate and comply with in practice. Example areas of particular interest to Schibsted are advertising and sentiment analysis for editorial insights.

High-risk AI

We agree with the Commission's proposal for special requirements being put on high-risk AI, but call for a number of clarifications also in this domain.

Categories of high risk AI

The proposal outlines – in Chapter 2, Article 9 – the need for risk management systems in relation to high-risk AI systems. The first step in this process is:" *identification and analysis of the known and foreseeable risks associated with each high-risk AI system*." The proposal defines "reasonable foreseeable misuse" as: *"the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems.*" However, this definition is unclear and somewhat circular in nature. This kind of language is unhelpful in clarifying what kinds of risks related to what kinds of misuse providers of high-risk AI systems would actually be liable for. Is it reasonable to assume that a person could fall asleep at the wheel of a self-driving car? Is it reasonable to assume that someone might use facial recognition technology to spy on their neighbors? We believe that the parameters of what constitutes reasonable foreseeable misuse require a high degree of specification to ensure there is no misunderstanding as regards liability and responsibility for these systems and the risks associated with them.

Further, we are of the opinion that the proposal around biometric identification can prove very hard to navigate in practice and **call for additional clarifications regarding the scope of such biometric identifications.** In the proposal, a remote biometric identification system is

defined as “an AI system for the purpose of identifying natural persons at a distance [...] , and without prior knowledge of the user of the AI system [...]”. We wonder whether “at a distance” combined with “without prior knowledge” practically leads to the definition being only applicable for biometric identification on public spaces, or whether “at a distance” could still refer to an AI system running on a natural person’s device?

Requirements related to high risk AI

Another area that needs further clarification relates to the potential for the regulation to unduly impact smaller players in terms of their ability to innovate in the field of high-risk AI. While the proposal outlines measures to assist SMEs with innovation, we would like to see additional clarification on how the ability to innovate will be secured for players larger than SMEs but smaller than global tech giants. There are many companies that do not meet the Commission’s criteria for an SME, but that do not have nearly the employees, resources or capabilities of the tech giants when it comes to ensuring that innovation efforts do not suffer as a result of compliance with regulations. **Safeguards must be included to ensure companies in this category are not put at a disadvantage in this respect.**

We believe that data quality is an important cornerstone for fair and effective AI and in principle welcome the proposed data governance measures of Article 10. We would still want to point out that, especially to the extent that AI systems are trained with data provided by natural persons, the requirement of ‘error free data’ can be disproportionate compared to the risks posed by the AI system. **We call for clarification on the requirement of ‘error free training data’ and suggest that the possibility to tie the requirement to the risks of the specific data attributes pose is investigated.**

Transparency

We applaud the Commission’s ambitions around transparency and **call for more clarity in regards to when the various proposed obligations shall apply**. In particular, we question whether any use of AI could ever be considered *‘obvious’*.

As the transparency requirements apply to all types of AI systems, it is important that it is sufficiently clear from the regulation in which situations or context transparency should be provided. Is ‘*interaction with natural persons*’ meant to be narrowed only to situations where a natural person might otherwise be thinking that they are interacting with another natural person? Or would it also cover situations where the interaction is more one-sided (e.g. AI based search engine, or AI-powered recommendations).

Beyond these fundamental questions, **we call for clarifications as to how informing of AI use towards natural persons should be carried out in practice.** As an illustrative example, we wonder if a single in-app notification complies with the proposal, or if users must be informed every time they are using a given AI service?

In regards to manipulated content, we **call for clarifications around the liability of sites with user-generated content** and ask whether the proposed transparency obligations fall on the user or the platform.

Schibsted

From a journalistic perspective, we consider how transparency obligations in the public sector should be expanded to include *all* (not just high risk) AI systems. In order to empower citizens and strive for an informed European public, **we suggest that all public sector use of AI should be listed in a public database.** As only high risk AI currently is subject to specific documentation requirements, this proposition of an additional step towards public sector transparency would require further details on what information should be included.

Regulatory sandboxes

The proposal outlines several measures to assist with this SME innovation, such as an AI regulatory sandbox designed to reduce the regulatory burden on and support SMEs. We welcome these, though further specification would be beneficial to ensure comparatively smaller players have the resources and guidance they need to innovate effectively.

It is crucial that the regulatory frameworks in the EU support innovation and test & learn-mentality, and we thus agree with the proposed formalisation of AI regulatory sandboxes. We would welcome the wider applicability of article 54 on further processing of personal data. **We propose an addition to 54 (1) (a) for AI solutions that promote transparent and democratic societal development and freedom of speech.**

Level playing field through enforcement clarity

We agree with the Commission's approach not to create a GDPR style one-stop-shop for AI enforcement. We suggest that the following two principles be promoted in the enforcement of the AI regulation:

1. **The actors who invest into compliance must benefit and not be disadvantaged by their investment.**
2. **Enforcement mechanisms must not lead to actors benefitting from establishing themselves in a specific Member State to avoid regulatory scrutiny.**

Requirements and liabilities for third party involvements must be clarified and easy to follow in practice. Open source development is common in the field, and to enable collaborative innovation within and beyond Europe, any obligations related to engaging in such should be clearly stated and easily understood by practitioners.

Finally, we are concerned by how different sectors and regions will interpret the obligations in highly varied ways – ultimately risking detrimental local approaches/cultures and therethrough an unbalanced playing field. **The proposal must safeguard against 'AI havens' where the ambitions for trustworthy AI are not prioritised.**