bitkom

Position Paper

2024 December

Bitkom views on data protection issues relating to the development and the use of Artificial Intelligence (AI)

Preliminary remarks

Artificial Intelligence (AI) is one of the key technologies of the future, with the potential to address long-term social and economic challenges. It offers transformative opportunities in areas such as healthcare, education, mobility and the digitalisation of processes both in the private and public sectors in general. However, we need to bring together/innovation and fundamental rights such as data protection. The EU needs to find a way to reconcile the freedom to conduct business (Article 16 CFR) with the rights of its citizens and the broader public interests of AI-driven progress. Striking this balance is crucial to fostering both a dynamic digital economy and a society where individual freedoms are respected.

The further development and use of AI is essential to ensure Europe's competitiveness. However, we are currently concerned that Europe is already falling behind other regions of the world, such as North America and Asia. The Mario Draghi report warns of the potential risks of declining European competitiveness in a context of slow growth. Legal certainty and clarification – like on the overlap between the AI Act and GDPR – is urgently needed to avoid Europe falling behind. It is crucial that the EU is able not only to develop AI technologies, but also to provide a regulatory framework that acts as a springboard for responsible and competitive AI innovation and use cases.

EU companies still have the opportunity to become AI leaders in their industries. In particular, the potential of AI for small and medium-sized enterprises (SMEs) is considerable. SMEs are the drivers of digitalisation, but they face an overly complex regulatory environment. Data protection, which rightly plays an important role in harnessing innovation for the societal good, should not be a barrier but an enabler of

progress. To tackle the challenges of AI, the European Union needs a coherent, innovation-friendly approach that takes into account economic interests, while maintaining a high level of protection of fundamental rights.

AI models, especially large language models (LLMs), operate on large amounts of mathematically abstracted data. While the process of training an AI model and generating outputs involves personal data, the model itself does not store personal data in its original form. Unlike databases, which store individual data points in a structured way, an AI model processes so-called embeddings – numerical representations that show patterns and relationships derived from the training data.

When considering the privacy implications of AI, it is therefore important to focus not on the model itself, but on three distinct phases of the AI lifecycle: (1) the development of the AI model; (2) storing the trained AI Model and (3) its deployment in various applications, where there is greater potential for harm but also for safeguards.

Privacy-enhancing-technologies should be built into the development process from the outset. Research frontiers are being pushed every day, and many companies are already implementing measures such as differential privacy, federated learning, confidential computing and data minimisation mechanisms. Practical and proportionate privacy safeguards can allow data subjects to exercise their rights while enabling innovation. Transparency about how models work and how they are trained is also essential to build trust and ensure regulatory compliance throughout the AI chain.

Challenges for data protection compliance in the context of developing and using AI

1. **Legal uncertainty concerning the applicable legal basis**
   The GDPR provides 6 different legal bases for processing of personal data, but not all of them are suitable for companies developing or deploying AI systems. In particular, consent requirements (Article6 (1)(a) GDPR) are difficult to implement in practice when developing AI models. AI training requires large, heterogeneous amounts of data, often from the open web and licensed sources, where it may not be possible to secure valid consent from all potentially affected data subjects. Businesses therefore need to be able to rely on compliant yet practical alternatives, such as the use of legitimate interest (Article 6 (1)(f) GDPR). Generally, developers are not seeking to process personal data or trying to identify specific data subjects. Training datasets for foundational models are large, unstructured, and generally only contain incidental personal data. Developers have a legitimate interest in developing high quality and performing AI systems, improving products and services for customers while mitigating bias and ensuring model safety. The use of personal data in AI training requires clarification of the requirements at the heart of the legitimate interests balancing test. The balancing of interests must also take into account the societal interests arising from the responsible development and deployment of AI. It is important to reaffirm Recital 4 of the GDPR, which provides that the processing of personal data should be designed to serve mankind.

2. **Lack of transparency and participation**
   The GDPR Article 64 (2) procedure for the European Data Protection Board (EDPB) to opine on the development and the use of AI is not sufficiently transparent, does not sufficiently involve the business community and does not take into consideration the multiple actors involved in AI systems, each with different levels of control over the data and decision-making processes. Greater involvement of companies of all sizes and industries in the development of EDPB guidelines and opinions is essential to achieving a common understanding of the privacy challenges that AI poses, and to find practical ways to comply with data protection principles while fostering innovation and competitiveness. A public consultation process, with the opportunity for business stakeholders to input and comment, should be made mandatory at an early stage. Rejection of comments must be justified and made understandable in order to increase the transparency and legitimacy of such processes.

3. **Challenges for SMEs**
   Companies of all sizes must respect the right to data protection. However, complex data protection regulations strain the resources of SMEs. Without pragmatic solutions and targeted support, SMEs, as key players in driving the EU's economy as well as its digitalisation, may be excluded from technological developments or their level of data protection compliance may be significantly reduced. The creation of one-stop-shops and clear, feasible-guidelines is urgently needed to reduce the burden on SMEs and facilitate their access to AI technologies.

Recommendations

1. **Clarification of the legal basis and other key data protection requirements concerning the development and the use of AI during those different stages: 1. Training, 2. Storing the trained AI Model and 3. Deployment of the Model**
   Clear guidelines on how to apply the requirements of the GDPR in the context of the development and the use of AI are urgently needed to dispel legal uncertainty. However, it is also important to emphasize that such guidance must be developed in the context of an open exchange under the governance of the EU AI Office to consider all views, including with the business community, in order to arrive at compliant but practical and workable solutions. Different safeguards would apply at different stages.

2. **Promotion of transparency and participation**
   The introduction of mandatory consultation processes for the European Data Protection Board with the business community at national and EU level would ensure that the regulatory process is practical and responsive to rapidly changing technology. The EDPB should develop guidelines with an appropriate comment period and on the basis of extensive stakeholder discussions to reflect the diversity of use cases. The EDPB should also promote understanding of AI technology and focus on technical considerations in addition to legal aspects. This is essential to provide a common baseline understanding for the subsequent legal assessment of the processes.

3. **Technological support and Standards**
   Policymakers should incentivize companies in a proportionate way to use privacy-enhancing technologies such as differential privacy, confidential computing, and federated learning to minimise privacy risks. Additionally, developers and deployers should implement safeguards, where appropriate, like data de-duplication and output filtering to minimize inadvertent personal data exposure, balancing innovation, and data protection. Standards need to be set and applied to both large and small companies and should be tailored to the typed of data processing and use cases (e.g. AI developers and deployers may need to follow different standards). An open platform for best practices could also provide effective support for companies.

4. **Specific measures for SMEs**
   Targeted funding programs and support for SMEs must be part of the EU's digital strategy. Particular attention needs to be paid to sector-specific challenges and solutions to make it easier for SMEs to start using AI.

Conclusion

In the current geo-political landscape, the European Union cannot afford to fall any further behind in the development and use of AI. This would cost the EU not only its economic competitiveness and sovereignty, but also its the ability to promote our technological standards and values globally. It is crucial that our regulatory framework protects the fundamental rights of citizens while enabling innovation.

Bitkom therefore calls for 1) greater industry involvement, 2) the promotion of technological solutions to data protection compliance challenges and 3) legal clarification to ensure that the development and use of AI in Europe. Responsible and sustainable AI requires a balanced framework that considers the interests of both businesses and individuals. This is the only way to ensure that AI becomes a driver of innovation that benefits all social and economic players equally.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Isabelle Stroot | Policy Officer for Data Privacy

T 030 27576-228 | l.stroot@bitkom.org

Janis Hecker | Policy Officer for Artificial Intelligence

T 030 27576-239 | j.hecker@bitkom.org

Responsible Bitkom committee

AK Datenschutz und AK Artificial Intelligence