Lernende Systeme
GERMANY'S PLATFORM FOR ARTIFICIAL INTELLIGENCE

Unlock the wealth of data while protecting privacy with AI

White Paper

Müller-Quade, J., Houdeau, D. et al.
Working Group for IT Security, Privacy, Legal and Ethical Frame

Executive Summary

Summary

Artificial intelligence offers enormous opportunities for innovative business models, for strengthening our coexistence and for ecological sustainability. Its potential is based on a constantly growing volume and availability of data, including sensitive data. But how can this treasure trove of data be turned into successful AI applications? According to a representative study (Bitkom Research 2021), only 13 % of German companies are currently using this data potential. The reason for this is the existing data protection regulations, which are often uncertain in their legal interpretation and thus impede the use AI on a broad scale. The white paper provides a solution-oriented perspective on this area of tension between data treasure and data protection, which combines data protection and a more flexible use of data. The paper calls for the legal recognition of technical privacy approaches based on European values to strengthen legal certainty for companies when using and developing AI. Precondition: there is no alternative to the use of personal data and it is in the common good.

Interactive field of data protection and public welfare-oriented data use for AI systems

The basis for common good achievements is the dataset that is required when using AI technologies for training Machine Learning models: patient health data, for example, could be used to facilitate and optimize the detection and treatment of diseases; movement data from people and vehicles could be used to reduce resource consumption. In public administration, the automation of administrative processes with personal data could make everyday work increasingly easier. All of these data sets are already available and are growing steadily as reality becomes increasingly digitalized. However, using these data sets for AI systems is complex, especially when it comes to personal data. As a result, companies face numerous challenges when dealing with data protection issues relating to personal data: Consent – yes or no? Is it necessary? How long should it be kept? How should personal data that flows into a company's circular economy be handled? The General Data Protection Regulation (GDPR) places high demands on the use of personal data. The implementation of data protection requirements in the context of data use for AI also shows that the legal interpretation is sometimes very uncertain. This causes many companies to shy away from the use and development of AI systems, meaning that the potential of this treasure trove of data is not fully exploited. In order to be able to close this currently existing freedom of interpretation in the processing of personal data, application-specific scope for action must be created by legislators and technical procedures for safeguarding data protection must be legally permitted. This requires both technical innovations to minimize legal uncertainties and targeted, application-specific legislation.

Figure: Data protection requirements for AI systems and interpretation in the application throughout the data lifecycle

Phase in the data life cycle	Legal data protection requirements	Uncertainties in application
Data collection	· Consent of the data subjects (Art. 4 No. 11 GDPR) · Informed consent of the data persons (Art. 6 para. 1 lit. a) GDPR) · Purpose limitation of the data collection (Art. 5 para. 1 lit. b) GDPR)	· How detailed needs the consent to be? · What degree of information is required? · How should purpose limitation be interpreted?
Data processing	· Principle of data minimization (Art. 5 para. 1 lit. c) GDPR)	· Data minimization makes secondary use of the data sets difficult
Data analysis	The following applies to automated decisions · Notification obligation pursuant to Art. 23 para. 2 lit. f) and Art. 14 para. 2 lit. g) GDPR, as soon as persons are affected by automated decisions in accordance with Article 22 GDPR · Right to information pursuant to Art. 15 para. 1 lit. h) GDPR · Right to object pursuant to Art. 21 para. 1 GDPR against the use of data	· When does an AI system fall under the legal definition of "automated decisions"?
Data publication	· Principle of purpose limitation (Art. 5 para. 1 lit. b) GDPR) · Lawfulness of the processing (Art. 6 para. 1 GDPR) · Declaration of consent that can be revoked at any time of the data subject (Art. 6 para. 1 lit. a) GDPR)	
Data storage	· Retention/deletion periods (Art. 17 GDPR) · Identification of data subjects only permitted for as long as the original data processing purpose requires it	· Scope for interpretation in the legal practice · Inconsistency in retention/deletion periods · Difficult to anonymize marginal groups · Semantic segmentation creates personal reference
Data secondary use	· Secondary use of data without the consent of the data subject is permitted if it is "logical next step" or is in the interest of the common good (Art. 6 para. 1 p. 1 lit. f) GDPR)	· „Logical next step" offers scope for interpretation · Interest of the common good is not clearly defined

Technical approaches to data use in the common good while protecting data privacy

Thinking about the conflicting priorities of data protection and data use as a symbiotic connection creates the prerequisite for a flexible, privacy-preserving use of data for and with AI in the common good. Various technical approaches can be used along the data life cycle. **Anonymization and pseudonymization measures** can be used to eliminate the personal nature of data as early as the data collection stage, meaning that the GDPR would no longer apply. The anonymization process promises complete elimination, while pseudonymization retains a certain degree of personalization. However, both technical processes significantly reduce data quality. Data synthesis, on the other hand, generates synthetic data sets that are not personal and, according to the current legal interpretation, do not fall under the GDPR and can therefore be shared publicly. However, their practicability is limited: high generation effort; not suitable for industries that rely on statistical features that enable personal identifiability to train their ML models. The differential privacy method, on the other hand, "blurs" data so that individual data points are no longer identifiable. This is particularly relevant for securing training data. But the practical implementation of differential privacy in real time and with small data sets is still problematic. **Cryptographic measures** also offer various options for safeguarding data protection. They start in the data life cycle during data processing in order to eliminate personal data. Due to the high computing load for the provision of model training, they are weaker in terms of scaling. As encryption measures, homomorphic encryption and secure multiparty computation guarantee input and output privacy but may be impractical in many application areas due to computational load and communication costs. Confidential computing as another cryptographic method closes an encryption gap in cloud computing and enables the secure processing of data in a trusted environment. This strengthens trust in data protection, but also requires communication costs. When it comes to data analysis for the specific training of AI models, the focus is primarily on **decentralized ML methods (Machine Learning)** to combine data protection and data use for the common good. With distributed ML, ML models are not trained on a central server, but on the end devices of the people providing the data. Their use therefore promises high data quality and a high degree of individual data sovereignty and is of particular interest to AI developers. These include methods of distributed Machine Learning and hybrid approaches to distributed Machine Learning. The latter promise to be able to close new attack vectors, maintain performance and at the same time guarantee data protection and security.

In addition to centralized and decentralized ML methods, procedures such as **Explainable AI (XAI) or Safe AI** could also be used as accompanying options to make the decisions and results of AI models more interpretable or comprehensible for the user ("painting the black box white"), thus increasing acceptance for the use of personal data for AI systems. **Data access management systems** such as data trustees or personal information management systems (PIMS), which also cover several phases of the data lifecycle, also offer an innovative approach to data usage flexibility in compliance with data protection regulations. Their approach to privacy-compliant data use is based on integrated data management within the data economy, which gives data subjects a more active and equal role in their data use for AI development and application.

The various technical and non-AI model-related technical measures offer the opportunity for data protection-compliant data use for AI systems in the common good across the individual phases of the data lifecycle. Against the background of their different performance capabilities in terms of accuracy, communication effort, computing load, data management and invasiveness in relation to data integrity, careful consideration and selection of the appropriate measure in the respective application context must be carried out. Above all, however, it is crucial that these measures are legally recognized in order to resolve existing uncertainties in the interpretation of the GDPR.

Regulatory options and outlook

A modern and functional legal framework for the flexible use of data in the common good that respects data protection must allow and promote those instruments that help to reduce uncertainty in the interpretation of the law and at the same time comprehensively protect conflicting rights and legal interests. This is based on a **technology-neutral data protection legal framework** that defines application-oriented and clearly interpretable requirements specifically for the use of data for AI systems to create legal certainty and certainty of action for AI development. This technology-neutral data protection legal framework based on a holistic approach and the possibility of adjustments to technical measures in the sense of "privacy by design" should also be enriched with further adjustments to the use of data for AI technologies in the proven interest of common good. **A uniform, broad-based definition of the common good** would be fundamental to be able to define the common good in a legally secure manner along specific application contexts with a clearly defined framework of criteria and, if necessary, to enable data use flexibilities. **A fundamental legal recognition of flexible data use** in the common good in the existing data protection legal framework is essential for this, which also **defines the legal consequences of flexibilization** in order to ensure certainty for data processors and guidance for data subjects. **Technical measures for the anonymization of personal data should therefore be standardized and certified** in order to support the flexibilization of data use. Preferably, the availability of non-personal data should be strengthened. Otherwise, if there is no alternative to the use of personal data, there is a **need to strengthen and legally recognize privacy by Design, data sovereignty and the data competencies of the data subjects themselves.**

The results of the analytical part were also presented in three use case scenarios from the areas of mobility (LEASYNG application scenario), education (learn.digital application scenario) and health (vAItality application scenario) to illustrate the central message in a compact form: Data protection and a more flexible use of data must be considered together in order to ensure legally secure room for manoeuvre for companies!

Imprint
Editor: Lernende Systeme – Germany's Platform for Artificial Intelligence | Managing Office | c/o acatech |
Karolinenplatz 4 | D-80333 Munich | kontakt@plattform-lernende-systeme.de | www.plattform-lernende-systeme.de |
Follow us on X: @Lernende Systeme | LinkedIn: de.linkedin.com/company/plattform-lernende-systeme |
Mastodon: social.bund.de/@LernendeSysteme | Status: October 2023 | Photo credit: sdecoret/Adobe/Title |
Translated using DeepL.com

This executive summary is based on the white paper *Datenschatz für KI nutzen, Datenschutz mit KI wahren: Technische und rechtliche Ansätze für eine datenschutzkonforme, gemeinwohlorientierte Datennutzung*. Munich, 2023. The authors are members of the working group IT Security, Privacy, Legal and Ethical Framework of Plattform Lernende Systeme. The original version of this publication is available at: *https://doi.org/10.48669/pls_2023-5*

SPONSORED BY THE

Federal Ministry
of Education
and Research

acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING