



Privacy Matters: Unlock the Power of AI Without Compromising on Privacy

Deloitte's AI privacy tool De-Identify anonymizes both categorical and continuous tabular data and evaluates the effectiveness of those measures in managing re-identification risk.

The Need

Artificial intelligence (AI) is rapidly evolving and has the potential to transform various industries and businesses. AI requires data, often in copious amounts, to function efficiently. The more granular the data, the better the algorithms can learn and make accurate predictions. Data collection has proliferated in recent years. Companies have come to value data as an asset and learned how to monetize it. Like any valuable asset, bad actors have an incentive to steal it. More than an economic loss, stolen data can become a liability for the company. Embarrassing data breaches and costly cyber-attacks require re-thinking how to create value with data while maintaining privacy.

Anonymized, pseudonymized and synthetic data have gained prominence as approaches for dealing with data risk, not only safeguarding the privacy of individuals but encouraging more data subjects to willingly provide their details, thus helping to train AI. Several techniques may be employed to protect the privacy of individuals within datasets. Traditional approaches focus on data masking or content obfuscation through encryption, hash function, and tokenization. However, not all anonymization techniques are equally effective. The risk of re-identification remains. Companies need a reliable methodology to assess the adequacy of their privacy risk management measures. Advanced anonymization

techniques, such as differential privacy, improve upon traditional masking methods by adding noise to the data. Combining such methods make it highly challenging to re-identify data subjects, while preserving the underlying distributions and patterns required to properly train a machine learning model.

Safely incorporating AI into processes, products and services is high on company agendas, and anonymization is a crucial component of that strategy. Whereas the importance and necessity of such objectives may be clear, how to achieve them is often less so. ➔

Our Solution: De-Identify

Deloitte's AI data anonymization and effectiveness assessment tool "De-Identify" provides a powerful, yet easy-to-use workflow for anonymizing both categorical and numerical tabular data. It enables users to both anonymize their data and assess the degree to which anonymization efforts successfully prevent re-identification.

De-Identify offers a wide range of methods for anonymization, including standard masking strategies such as data substitution, suppression, and generalization. It provides differential privacy anonymization by applying randomization using Laplace or exponential noise. De-Identify also enables deterministic masking and the preservation of correlation, facilitating the anonymization of data while preventing re-identification with minimal loss of expressiveness.

Furthermore, De-Identify provides multiple, advanced privacy metrics to evaluate the level of anonymization and reduce the risk of re-identification without requiring the original, adding to the tool's versatility in protecting data privacy.

Advantages/Benefits of De-Identify

- Examines privacy from multiple perspectives by assembling a collection of privacy indicators
- Uses both masking and differential privacy anonymization strategies
- Highly accessible to business users via the graphical user interface and straightforward, intuitive workflow
- Provides a means to generate synthetic data using anonymization techniques.

Example Use Cases

- Sanity checking anonymization efforts by providing immediate feedback
- AI model validation for adherence to trustworthy AI principles
- Helping fulfill conformity to privacy compliance laws GDPR and AI Act
- Generation of representative synthetic data

Contact

David Thogmartin

Leader aiStudio
dthogmartin@deloitte.de

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.