PRIVAGAMS – Services for Privacy Advancement through Generative AI and Model Sanitisation

OSCARS
Open Science Clusters' Action for Research & Society

PRIVAGAMS creates a cutting-edge platform for generating privacy-preserving simulated data using Diffusion Models. It ensures high-quality, realistic datasets while protecting sensitive information, with applications in clinical, tabular, and imaging data. The project also focuses on sanitising machine learning models, through advanced techniques, such as model distillation and watermarking, enabling secure research across various RIs.

LS RI
Life Sciences

Challenge

Ensuring privacy while maintaining data utility is a growing concern, especially in sensitive fields like healthcare. Current anonymisation techniques struggle to preserve critical relationships within data, while machine learning models can inadvertently retain sensitive information, potentially exposing private data.

Solution

A platform enabling research institutions to produce high-quality simulated data customised for specific needs, thus increasing data availability while ensuring privacy remains intact. The project will do so by utilising GANs to create simulated datasets that closely mimic real data without exposing personal information.

Scientific Impact

By allowing the generation of privacy-preserving yet realistic datasets, the platform enables institutions to share data more freely without compromising privacy. Its model sanitisation techniques secure machine learning models against data leakage.

Partners

Medical University Graz (coordinator), Masaryk University, Technische Universität Wien, Biobanking and Biomolecular Resources Research Infrastructure – European Research Infrastructure Consortium - BBMRI-ERIC, Masaryk Memorial Cancer Institut

https://www.oscars-project.eu/projects/privagams-services-privacy-advancement-through-generative-ai-and-model-sanitisation