OSCARS
Open Science Clusters' Action for Research & Society

Funded Project

PRIVAGAMS - Services for Privacy Advancement through Generative AI and Model Sanitization

Presenter: Robert Harb, Medical University of Graz, ORCID: 0009-0001-3427-7054

Implemented by

Med Uni Graz

TU WIEN

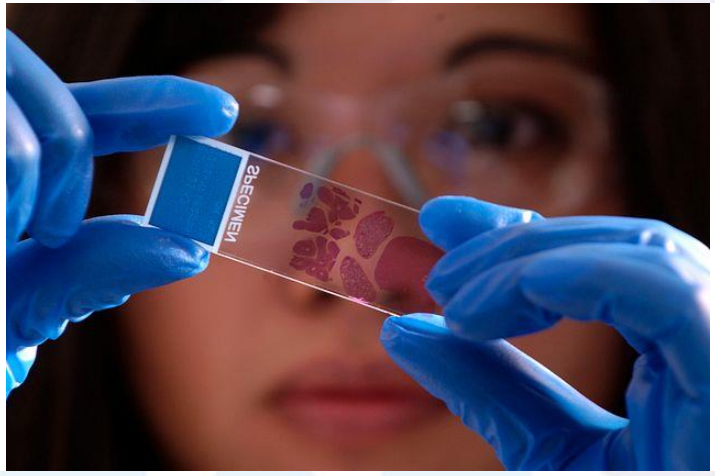
MASARYK UNIVERSITY

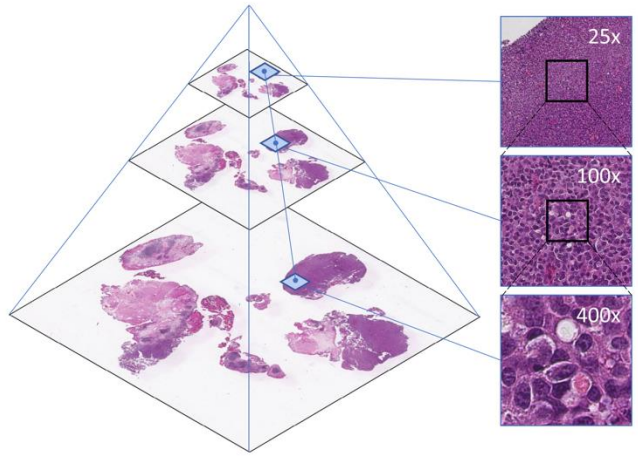
Masaryk Memorial Cancer Institute

Funded by the European Union

What problem(s) are you going to solve?

- Digitization allows large-scale scanning of tissue samples in **Pathology**
- The Biobank in Graz alone holds **over 20 million** glass slides
- These images are an **invaluable resource** for advancements in medicine and AI
- Strict legal frameworks **limit data sharing**, to protect patient privacy
- To foster **Open Science**, we need methods to make data publicly available





What are you planning to do to solve the problem?

- Generative AI can produce realistic **synthetic** pathology **images** [1]
- Synthetic images that lack identifiable patient details enable **sharing without compromising privacy**

Our goals are:

- **Sanitization** and **differentiable private training** of models
- Implementing a framework that **assess privacy preservation** by evaluating the susceptibility to linkage attacks [2]
- Organize an international **competition** on privacy attacks

[1] Diffusion-based generation of histopathological whole slide images at a gigapixel scale, WACV 2024, Harb et. al.
[2] Privacy risks of whole-slide image sharing in digital pathology, Nature Communications 2023, Holub et. al.

What will be the results and how do you plan to make them available to the broader community?

- **Privacy-Preserving Models**: Open-source generative models that retain clinical details while safeguarding patient privacy
- **Practical Guidelines**: Procedures for data preparation, training, and evaluating privacy-preserving models
- **Synthesized Histopathological Images**: privacy-safe images available for medical researcher and AI model development

What risks could limit the success of the project, and how can they be mitigated

- Privacy-preserving generative modeling is an **emerging field**, with limited established best practices
- Advanced linkage attacks could **uncover real patient identities** if the generative model inadvertently retains identifiable features

OSCARS

Who is doing it?

Medical University Graz

Robert Harb

Heimo Müller

Technical University Vienna

Bernd Saurugger

Andreas Rauber

Masaryk University Brno

Jakub Pekar

Petr Holub

Vit Musil

Masaryk Memorial Cancer Institute

Rudolf Nenutil