NARODOWE CENTRUM NAUKI

Institution	Institute of Computer Science, Polish Academy of Sciences
Job type	Employment contract, post-doc position
Project	Privacy and data ownership meet generative neural networks financed within NCN OPUS grant No: 2023/49/B/ST6/02580
Project leader	Paweł Morawiecki
Description	The project lies at the intersection of privacy, security and machine learning. In recent years, there have been rapid advances in generative modeling techniques within the field of deep learning. Among these, generative diffusion models, particularly those utilizing the Stable Diffusion framework, have gained prominence due to their capability to generate high-quality, diverse, and intricate samples. These models hold considerable potential for numerous applications, such as data augmentation, art creation, and design optimization. However, as these models become more widely adopted, addressing privacy and data ownership concerns becomes essential. Recently, Getty Images filed a lawsuit against Stability AI, accusing it of unlawfully copying and processing millions of copyright-protected images. One critical issue that arises in this context is determining whether a specific data point was used during the training process of a model. Extracting this information from a model can be crucial in cases where copyrighted or sensitive data are used without permission, leading to potential legal issues. The importance of these matters is reflected in the European Union General Data Protection Regulation (GDPR), particularly Article 17 often referred to as the "right to be forgotten". In this project, we want to investigate whether it is possible to infer meaningful information on training set for big, real-life generative neural networks. We also are interested in unlearning (forgetting) a given image to ensure that the neural network is no longer able to generate a very similar image or its style. Such a precise forgetting, if successful, would allow a user to be forgotten/withdrawn from the service without the need to retrain the whole network.
Salary	140 000 PLN per year, gross
Maximum period of contract	2 years
Application deadline	15th September 2024
Decision	up to 1st October 2024
Position starts on	1st October 2024
Profile of a good candidate	Ph.D. in mathematics or Computer Science(obtained up to 7 years from the date of employment), actively working in machine/deep learning (confirmed by publications in international conferences/journals), practice in computer programming, experience in using the deep learning frameworks such as

	Tensorflow or/and PyTorch
Key responsibilities	contributing ideas and technical solutions for research on membership attack and 'forget mechanism' for generative models, implementations of neural network models in PyTorch/Tensorflow
Required documents	CV list of publications and research projects document confirming the scientific degree (copy of the PhD diploma)
Please submit the documents to:	pawel.morawiecki@gmail.com