



How emerging technologies enable trustworthy data sharing

PD Dr. Andreas Trügler Know-Center, University of Technology and University of Graz

01.03.2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481

Encryption and data sharing?





How to collaborate?





Homomorphic Encryption





Private Set Intersection





How does it work?



(1) Encrypt data with private key



(2) Exchange encrypted data sets



(3) Encrypt again with private key...



(4) Compare double encrypted values



What challenges are there to overcome?



- Performance bottlenecks
- Algorithms are still under development...
- Legal framework within the European Union







Our Contributions in TRUSTS



Multi-Party Computation under GDPR





What is comming next?



- Upscaling and further improving perfomance
- Handling of more complex scenarios (e.g. MK-FHE)
- Encrypted federated machine learning
- Transformation of algorithms to privacy-preserving certified
- Legal assessment of cryptographic solutions



Thank You





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481