Reykjavik University and Frostbyte Research Centre

National Coordination Centre for Cybersecurity in Iceland (NCC-IS/Eyvör)

Defend Iceland

Dr. Fatima Zahra Errounda, Assistant professor @ Reykjavik University, Iceland (https://scholar.google.com/citations?user=iT6CjvsAAAAJ&hl=en&oi=ao)

Area of expertise: Differential privacy, federated machine learning, law and technology gaps

*Frostbyte research centre (*https://www.frostbyte.is/*)*: co-funded by the European Union and European Cybersecurity Competence Centre

Collaborator on NCC-IS

Fatimae@ru.is

COMPASS: COMpliant Privacy-Aware Secure Systems (SecureAI)

Impact:

- Unifies technical PET, regulatory fit, and organizational readiness into an operational governance system

Activities:

- Framework that maps privacy and security risks across the AI lifecycle
- Implement security controls around AI systems

Use cases:

- Healthcare, education, legislators and law firms

Description of Desired Consortium

Complementary skill still needed for the proposed consortium:

- Privacy law experts
- Governance and policy experts
- Domain experts
- Security and privacy experts

Collaborators, Frostbyte Research Centre

Dr. Fatima Zahra Errounda
Differential privacy
Privacy threats
Federated learning
Law and technology

Dr. Jackqueline Mallet
Cybersecurity
Computer networks
Penetration tests

Dr. Hans Reiser
Cybersecurity and AI
Distributed systems
Malware classification
Intrusion detection

Dr. Giovanni Apruzzese
Cybersecurity and AI
Threat modelling of AI-Driven systems