Title: *"Strengthening User Privacy through AI-Driven Risk Quantification and International Standards Alignment*

Aim: AI-based privacy quantification is an emerging but underdeveloped field. Existing works such as Polisis [2] and PrivacyBERT [3] automate privacy-policy analysis but remain disconnected from international standards and lack quantifiable indicators of user or system risk. Recent frameworks such as NIST's AI Risk and Privacy Frameworks [4] highlight the growing demand for measurable, interoperable privacy-risk metrics. However, no current approach integrates AI-driven privacy analysis with standards-based compliance measurement [1]. This project fills that gap by developing AI methods to quantify user privacy risks in line with ISO/IEC, NIST, GDPR and related regulations. It will deliver validated privacy metrics, a proof-of-concept tool combining PrivacyBERT and Bayesian risk modelling, and a roadmap for scaling into a comprehensive, standards-aligned framework which laying the foundation for stronger privacy protection, accountability, and trust.

Approach: The project will follow four delivery-focused steps. (1) Map measurable privacy principles from ISO/IEC, NIST, GDPR, IEEE and related regulations into quantifiable indicators by translating clauses such as consent, data minimisation, encryption, and third-party sharing into candidate metrics. (2) Design and test privacy-risk metrics at user, system, and organisational levels using synthetic logs and public breach datasets of ENISA [6] and PRC [7]. Organisation-level indicators (e.g., compliance time, vendor safeguards, breach response) will be partially implemented, while digital ecosystem issues (e.g., cross-border transfers and interoperability) will be scoped conceptually for future work. (3) Develop an AI prototype combining transformer-based model PrivacyBERT which is fine-tuned on OPP-115 dataset [5] and Polisis datasets [2] for clause classification with Bayesian/probabilistic models for privacy-risk scoring. These datasets provide annotated privacy policies widely used for training and evaluating AI models in privacy clause classification and compliance analysis. (4) Validate and refine the prototype through benchmarking against defined metrics, producing a validated tool and deliver final report.

Novelty and Expected Contribution: The project's novelty lies in combining transformer-based policy analysis, probabilistic risk modelling, and international standards mapping into a single comprehensive quantitative framework. The earlier studies classify privacy clauses or analyse breaches in isolation, this project will create the first standards aligned, multi-level privacy risk quantification model which advances the state of the art in AI enabled privacy assurance.

Timetable / Plan (4 Months)

Month	Activities	Deliverables

1	Map measurable privacy principles from ISO/IEC, NIST, GDPR, IEEE and international data protection regulations into privacy indicators.	International standards to privacy metrics mapping
2	Define and test user, system, and organisation-level privacy metrics, scope digital ecosystem level privacy indicators, and generate synthetic datasets.	Draft privacy metrics along with synthetic data
3	Build AI prototype using PrivacyBERT for privacy clause classification and Bayesian risk models for privacy risk scoring.	Prototype user privacy quantification AI tool
4	Test prototype on real/synthetic data, benchmark metrics, and deliver final report	Validated tool and final report

References:

1. Arshad R., Asghar R., "Characterisation and Quantification of User Privacy: Key Challenges, Regulations, and Future Directions", IEEE Communications Surveys and Tutorials, 2024.
2. Hamza Harkous, Kassem Fawaz, 2018. Polisis: automated analysis and presentation of privacy policies using deep learning. In Proceedings of the SEC'18. USENIX Association, USA, 531–548
3. Muralitharan, J., Arumugam, C. Privacy BERT-LSTM: a novel NLP algorithm for sensitive information detection in textual documents. *Neural Compute & Applications* 36, 15439–15454, 2024.
4. https://www.nist.gov/itl/ai-risk-management-framework
5. https://www.usableprivacy.org/static/data/OPP-115_v1_0.zip
6. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach
7. https://privacyrights.org/data-breaches