Title: Ensuring User Data Protection in Machine Learning Models

1. **Problem Statement**: Develop a privacy-preserving machine learning model for credit risk assessment in banking.

2. **Introduction:** Banks handle sensitive personal data, and it's crucial to ensure data privacy even when the data is used for machine learning tasks. This project will involve implementing a machine learning model for credit risk assessment while preserving the privacy of user data.

3. **Relevance**: As more stringent data protection laws come into effect worldwide, privacy-preserving machine learning will be crucial for banks to maintain compliance while gaining insights from their data.

4. **Data Source:** German Credit Data (https://archive.ics.uci.edu/ml/datasets/statlog+(german+credit+data))

5. **Weekwise tasks:**
    a. Week 1-2: Import and preprocess data. Conduct exploratory data analysis and understand the data structure.
    b. Week 3: Research and understand privacy-preserving machine learning techniques, such as differential privacy and homomorphic encryption.
    c. Week 4: Design a machine learning model for credit risk assessment while incorporating privacy-preserving techniques.
    d. Week 5-6: Implement and train the model using the dataset. Validate the model using appropriate performance metrics.
    e. Week 7: Test the privacy preservation of your model using various attack scenarios. Evaluate the trade-off between model performance and privacy preservation.
    f. Week 8: Write the final report and prepare the project presentation. The report should detail the methods used, findings, conclusions, and suggestions for future work.

6. **Evaluation Guidelines:** The project will be evaluated based on the effectiveness of the privacy-preserving techniques, the performance of the machine learning model, and the clarity of the final report and presentation. The project should include an evaluation of the trade-off between data privacy and model performance.

Here are five related GitHub repositories that can serve as a starting point for the "Ensuring User Data Protection in Machine Learning Models" project:

1. TensorFlow Privacy: TensorFlow Privacy is a Python library that includes implementations of TensorFlow optimizers for training machine learning models with differential privacy. It can be used for learning without memorizing sensitive data.
2. PySyft: A Python library for secure, private computation and federated learning in PyTorch. PySyft is designed to allow data to remain in the hands of its owner, while still permitting remote computations to be performed on it.
3. TensorFlow Federated: TensorFlow Federated (TFF) is an open-source framework for machine learning and other computations on decentralized data. This allows for user data to remain local while still training ML models.
4. PaddleFL: PaddleFL is a framework for federated learning. It is designed to support a wide range of machine learning tasks, while ensuring the protection of sensitive data.
5. IBM Differential Privacy Library: This library provides several tools to make differential privacy accessible to non-experts and improve its usability. It includes a wide variety of algorithms, which can help in preserving user privacy while conducting machine learning tasks.