Please be advised that the following serves as a guide. Teams are strongly urged to engage in thorough research concerning data privacy and protection. They have the flexibility to propose project ideas beyond those listed, as long as the suggested project aligns with the scope of data privacy and protection.

Thematic Areas

The code4privacy hackathon participants will be challenged to develop an ICT-based idea or solution that addresses one or more of the following:

1. **Early Integration of Privacy:** Participants are encouraged to conceptualize and build products or systems where privacy features are fundamental from the initial design phase.
2. **Innovative Privacy Technologies:** Explore cutting-edge technologies (such as homomorphic encryption, differential privacy, etc.) that enable data processing while maintaining privacy.
3. **User-Centric Privacy Solutions**: Emphasize solutions prioritizing user consent, transparency, and control over their data while delivering seamless experiences.
4. **Legal and Ethical Compliance:** Promote solutions that align with the Nigeria Data Protection Act and adhere to ethical data collection, storage, and usage principles.

Project Ideas

1. Build systems for Secure Data Processing:

Secure Data Processing refers to the development and application of techniques that enable the extraction of valuable insights from data while rigorously preserving the anonymity of individuals within that data. The objective is achieved through the integration of cryptographic and statistical methodologies, building tools that analyze data primarily with encryption and privacy-enhancing mechanisms like differential privacy and homomorphic encryption.

Action: Build systems that can process data while preserving the privacy of individuals, focusing on techniques like encryption.

2. **Decentralized Identity**: Decentralized identity (DID) refers to a model of identity management that enables individuals to control their digital identities without the need for a central authority or intermediary.

Traditional identity systems often involve centralized databases or authorities that store and manage individuals' personal information, creating potential risks such as data breaches, privacy issues, and lack of user control over their own data.

Action: Create a system where people control their own digital identity, sharing only what is needed with organizations, cutting down on data breaches.

3. **Privacy-Preserving Analytics:** Privacy-preserving analytics refers to the practice of analyzing data while simultaneously safeguarding the privacy and confidentiality of the individuals or entities associated with that data. It involves deriving insights, patterns, or valuable information from sensitive or voluminous personal datasets without revealing the raw, identifiable information of the individuals within the dataset.

Action: Develop methods to extract insights from anonymized data while protecting individual privacy, valuable for research and statistics.

4. **Privacy Browser Extension:** Privacy-preserving analytics refers to the practice of analyzing data while simultaneously safeguarding the privacy and confidentiality of the individuals or entities associated with that data. It involves deriving insights, patterns, or valuable information from sensitive or personal datasets without revealing the raw, identifiable information of the individuals within the dataset.

Action: Build an extension that scans websites for data collection practices, alerting users and offering tools to protect their privacy.

5. **Decentralized Identity Verification:** Decentralized identity verification involves confirming and validating an individual's identity using decentralized systems, where control over personal information rests with the individual rather than a centralized authority. This approach aims to provide secure and reliable verification while respecting user privacy and giving individuals greater control over their identity data.

Action: Design a system for secure and self-managed digital identities, allowing users to prove their identity without sharing unnecessary data.

6. **AI-powered Privacy Tools:** AI-powered privacy tools leverage artificial intelligence (AI) techniques to enhance and protect user privacy across various digital platforms and interactions. These tools utilize machine learning algorithms, natural language processing (NLP), computer vision, and other AI methods to provide users with improved control, security, and confidentiality of their personal data.

Action: Use AI to detect and prevent privacy threats, like image recognition for sensitive information or automated redaction of personal data.

7. **Privacy-Focused Social Network:** A privacy-focused social network is a platform designed to prioritize and protect user privacy while facilitating social interactions and content sharing among its users. These networks aim to offer alternatives to traditional social media platforms by focusing on safeguarding user data, providing enhanced control over personal information, and minimizing the collection and sharing of user data for commercial purposes.

Action: Create a platform that prioritizes user privacy, featuring end-to-end encryption, limited data collection, and user control over data sharing.

8. **Privacy Audit Dashboard**: A privacy audit dashboard is a centralized interface or tool used by organizations to monitor, assess, and manage their data privacy practices, compliance, and risks. It provides a comprehensive overview of an organization's data handling processes, allowing for the evaluation of privacy measures and ensuring adherence to relevant privacy regulations and internal policies.

Action: Build a tool that analyzes user data sharing habits, provides insights, and recommends actions to improve online privacy.

9. **Blockchain for Data Ownership:** Blockchain technology offers a promising framework for establishing and maintaining data ownership through its decentralized, immutable, and transparent nature. It enables

the creation of a secure and tamper-proof record of data ownership and transactions, providing individuals or entities with greater control over their data.

Action: Explore how blockchain can give individuals ownership and control over their data, letting them choose who accesses it and how.

10. **Privacy-Focused Mobile App:** A privacy-focused mobile app is a software application designed with a primary emphasis on protecting user privacy and data security while delivering its intended functionalities. These apps prioritize safeguarding user information, minimizing data collection, and providing users with greater control over their personal data.

Action: Develop an app that helps users secure their data and manage app permissions, offering granular control over what they share.

11. **Secure IoT Ecosystem:** A secure Internet of Things (IoT) ecosystem refers to a network of interconnected devices, sensors, and systems that prioritize robust security measures to safeguard data, ensure device integrity, and protect against potential threats within the IoT infrastructure. Securing the IoT ecosystem involves implementing measures at various levels to mitigate vulnerabilities and risks associated with connected devices.

Action: Design a system that ensures the privacy and security of data generated by IoT devices, allowing users to manage and protect their personal data.