Project One

CS370 – Current Emerging Trends

Benjamin Leanna

SNHU

2024 – 02 – 04

This white paper addresses concerns raised by an EU regulator regarding potential violations of GDPR principles by a major social networking company employing neural networks in personalization algorithms. The company aims to maximize user engagement and advertising revenue through tailored user experiences. The following sections provide an overview of neural networks, their role in personalization, an analysis of GDPR implications, and proposed adaptations for compliance, incorporating information from reputable sources.

**I. Basics of Neural Networks:**

Neural networks, inspired by the human brain, learn and make decisions. In personalization algorithms, they consist of an input layer, hidden layers for processing, and an output layer for classification. The input layer receives user data, and the hidden layers process it to generate personalized recommendations. The output layer produces classifications based on learned patterns (Capgemini).

**II. Neural Networks and Personalization**:

Neural networks process large datasets to predict user preferences, allowing the company to deliver personalized experiences. Ethical concerns arise due to the 'black box' nature of these algorithms, potentially leading to hidden biases. Users may not understand how recommendations are made, raising transparency issues (Business 2 Community).

**III. GDPR Implications on Personalization:**

*Transparency*: GDPR mandates clear communication of data usage. Enhancements in transparency, as suggested by ICO's guidance, should be implemented in algorithms to ensure users understand how their data informs personalization.

*Purpose Limitation*: GDPR emphasizes collecting data for specific purposes. The company must articulate precise goals of data collection, aligning them with providing personalized experiences (ICO).

*Data Minimization*: GDPR stresses collecting only necessary data. Regularly reviewing and limiting data collected to fulfill personalization objectives aligns with data minimization principles (ICO).

*Accuracy*: GDPR mandates data accuracy. Regularly updating user profiles and addressing inaccuracies aligns with GDPR requirements (ICO).

*Storage Limitation*: Data retention should align with defined purposes. The company must establish clear timelines for data storage, preventing indefinite retention (ICO).

*Confidentiality*: GDPR mandates robust data security measures. Employment practices outlined by GDPR-info.eu to ensure user data is secure and confidential.

*Accountability*: GDPR requires establishing accountability measures. Outlining responsibilities and potential penalties for non-compliance aligns with GDPR principles (ICO).

**IV. Legal Concerns and Alternatives:**

Legal concerns may arise regarding the 'black box' nature of neural networks. Users may question data collection practices. While not collecting data is not a feasible option for the company's business model, transparency enhancements, as recommended by TechGDPR, can address concerns and improve compliance.

**V. Proposed Adaptations for GDPR Compliance:**

*Current Trends in AI and Privacy Preservation*: As suggested by Medium, employing privacy-preserving AI techniques, like federated learning, can limit data exposure.

*Changes in Data Practices*: Enhance transparency in data usage, provide opt-in choices for users, regularly review and minimize collected data, and establish strict data storage timelines, aligning with GDPR (TechGDPR).

*Defending Existing Practices*: Maintain the core data-driven business model, emphasizing responsible data usage and ensuring user trust through transparent communication (Business 2 Community).

In closing, this white paper outlines the interaction between neural networks and GDPR principles, proposing adaptive measures to align with compliance requirements, incorporating insights from reputable sources. Balancing personalization with user privacy is essential for sustained success in the dynamic landscape of social networking.

Capgemini. (2023, September 4). *Expert perspectives - Capgemini*. https://www.capgemini.com/insights/expert-perspectives/

ICO. (n.d.). *UK GDPR guidance and resources*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

Spillane, J. (2022, December 8). *How GDPR Can Undermine Personalization and User Experience*. Business 2 Community.

Ved, A. (2023, April 19). *How to develop Artificial Intelligence that is GDPR-friendly*. TechGDPR. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/

Dorschel, A. (2021, December 9). Rethinking Data Privacy: The impact of Machine learning. *Medium*. https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

*General Data Protection Regulation (GDPR) – Official Legal text*. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/