Darren Sheftic

CS-370 Emerging Trends in CS

Prof. Binyam Heyi

7/24/2024

GDPR Compliance in Neural Network-Based Personalization

In today's digital world, creating personalized experiences for users is key to the success of social networking platforms. Our company uses neural networks to customize content, recommendations, and ads for each user. However, the General Data Protection Regulation (GDPR) by the European Union has raised concerns about how we handle data. This paper aims to address these concerns to ensure we comply with GDPR while continuing to provide exceptional user experiences.

Neural networks are inspired by the human brain and are an important part of modern artificial intelligence. They have three main parts: the input layer, hidden layers, and the output layer. The input layer receives raw user data, like mouse clicks and site navigation patterns. The hidden layers process the data through interconnected nodes called neurons, finding patterns within the data. The output layer generates personalized recommendations based on the processed data.

We continuously collect user data and feed it into neural networks. These networks analyze the data to identify patterns and make personalized recommendations. Neural networks can introduce biases in data and algorithms. These systems are often "black boxes," meaning users can't see how their data is used to make recommendations. Hidden biases may result in unfair outcomes.

The portions of the GDPR that affect personalization are transparency, purpose limitation, data minimization, and accuracy. We must clearly explain how we use user data. Data should only be collected for specific, stated purposes. Only the necessary data should be collected. User data must be accurate and up-to-date. (GDPR Info, 2018) We are responsible for following these rules and may face penalties for non-compliance.

Our current data practices may raise a few legal issues under the GDPR, such as Transparency and Data Minimization, Data Security, and Storage Limitation. Our extensive data collection may not be fully transparent to users, potentially violating GDPR requirements. Ensuring the confidentiality of user data is critical. Any breaches could result in severe penalties.We need to ensure that data is not kept longer than necessary. This means we must regularly review our data retention policies and delete data that is no longer needed, though this will be difficult for optimizing user personalization. However, failing to do so could result in legal penalties and loss of user trust. Considering our business model, limiting data collection may hinder our ability to provide personalized experiences and monetize through targeted advertising. However, aligning with GDPR principles is essential for maintaining user trust and avoiding legal repercussions.

There are potential adaptations we may use to maintain GDPR compliance using current trends and best practices. Techniques such as federated learning and differential privacy can help ensure compliance while still allowing for effective personalization (Dorschel, 2019).The company can utilize clear and transparent consent processes that can help meet GDPR requirements for transparency and user control (Spillane, 2022).Implementing user-friendly disclosures explaining how data is used for personalization will aid in transparency. This includes clear consent mechanisms. We can define and communicate specific purposes for data collection, ensuring data is only used for these purposes. We can regularly review data collection practices and limit data to what is necessary for personalization.We can establish procedures for regularly updating and correcting user data.We can develop and enforce data retention policies, deleting data when it is no longer needed.We can enhance data security measures to protect user data from breaches.We can appoint a Data Protection Officer (DPO) and conduct regular GDPR compliance audits. These practices will help our company maintain GDPR compliance in alignment with their principles.

Ensuring GDPR compliance is paramount for maintaining user trust and legal standing. By implementing the proposed changes, we can continue to deliver personalized user experiences while respecting user privacy and adhering to GDPR requirements.

**References**

Dorschel, A. (2019). Rethinking Data Privacy: The Impact of Machine Learning. Medium. Retrieved from <https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60>

GDPR Info. (2018). General Data Protection Regulation (GDPR). Retrieved from <https://gdpr-info.eu/>

Spillane, J. (2022). How GDPR Can Undermine Personalization and User Experience. Business 2 Community. Retrieved from <https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269>

Ved, A. (2019). How to Develop Artificial Intelligence That Is GDPR-friendly. TechGDPR. Retrieved from <https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/>