**Explain the Basics of Neural Networks and How They Work**

Humans can learn and understand complex, non-linear relationships in data. Consider a busy four-way intersection that drivers navigate daily. In the simplest case, pass through the intersection when the light is green, yield to yellow, and stop at red. However, these basic rules would be insufficient for a machine or new driver.

For instance, a self-driving car might follow these rules but encounter situations like an oncoming vehicle when turning left on green or an emergency vehicle crossing. Moreover, the traffic light might malfunction, providing no data to process. These scenarios require handling more than just the basic instructions, which is where neural networks come into play, helping artificial intelligence process complex data relationships (New York Institute of Technology, 2023).

Neural networks work through three layers: the input, hidden, and output layers. A useful analogy is a microwave. The input layer is like the food and instructions you provide before pressing start. The hidden layer represents the heating process where the food is transformed, and the output layer is the result—the heated food and the beeping that tells you it's done. Similarly, neural networks take in data (input), process it (hidden layers), and deliver results (output) (New York Institute of Technology, 2023).

**Evaluate How Neural Networks Are Used to Create Personalization**

Neural networks remain central to personalizing user experiences, despite increasing restrictions (Spillane, 2022). In a shopping app, for example, neural networks analyze user-specific data, such as preferred shopping times, frequently bought items, and location. After processing this data, the network personalizes the output, such as sending notifications at times the user typically shops or showing products based on past purchases.

However, unchecked use of these models can raise ethical concerns. Collecting user data might enhance the experience, but it can also manipulate users. Additionally, bias can infiltrate the models. For example, Amazon's hiring algorithm inadvertently favored male candidates because the input data contained more male profiles, leading the system to assume this was preferred (Denison, 2023).

A further concern is the opacity of these systems. Complex neural networks can become "black box" models, where even developers cannot explain how specific outputs are generated (Yasar, 2023). This lack of transparency exacerbates the challenge of addressing hidden biases within these models.

**Analyze How Portions of the GDPR Affect Personalization**

The General Data Protection Regulation (GDPR) severely limits how and when user data can be collected and used, which has dramatically impacted businesses relying on personalization. One key principle is transparency: companies must clearly inform users what data they collect and how it will be used (Richard, 2023). This restriction challenges businesses, as users might see targeted marketing as intrusive, even though companies view it as enhancing the user experience.

Another critical principle is purpose limitation, which mandates that data be collected only for explicitly stated and legitimate purposes (Richard, 2023). Businesses can no longer amass vast user datasets to reuse as they see fit; they must specify the data’s purpose and stick to it.

Data minimization complements purpose limitation, allowing companies to collect only the data necessary for their stated purposes (Richard, 2023). This aligns with the principle of least privilege: businesses can only collect what's absolutely essential for personalization, limiting the depth and scope of user profiling.

Finally, the accuracy principle ensures that companies strive to keep data up to date and discard inaccurate or incomplete data (Richard, 2023). These GDPR principles force businesses to rethink their data strategies to ensure compliance while maintaining effective personalization.

**Assess How the GDPR Is Affecting the Company’s Practices**

Collecting large amounts of data with few limitations allows companies to create highly personalized user experiences, which leads to higher engagement and purchase rates (Spillane, 2022). However, GDPR places businesses at significant legal risk if they fail to comply with the regulation's data protection standards. A striking example is JD Wetherspoons, a UK pub chain whose CEO deleted the entire customer mailing list to avoid GDPR-related penalties (Spillane, 2022).

As stated earlier, a neural network operating as a “black box” poses a significant issue as the GDPR demands transparency. If we are unable to define how our neural network makes decisions, we are at risk. Direct compliance with data collection must also be ensured to fit the necessary standards.

Retargeting customers has been directly affected through the GDPR’s right to be forgotten which gives users the right to request a business wipes the user’s data from their system. (Spillane, 2022)

Thus, understanding and adhering to these rules is essential. While GDPR restricts the use of data, it doesn't eliminate the potential for neural networks and algorithms—it simply defines boundaries. Avoiding data collection altogether is neither necessary nor feasible. Personalized experiences have been shown to significantly improve user engagement and ad revenue. Therefore, collecting user data is critical to maintaining the business model's success.

**Propose Adaptations to the Company’s Practices to Act in Compliance with the GDPR** Given the importance of personalization to the company’s business model and the constraints imposed by GDPR, we must adapt our data collection practices to remain compliant while maximizing user insights.

We need to align with GDPR transparency and purpose limitation, so our model must adjust to asking for explicit consent for any and all user data collection. Users should be given the option to consent to different types of data collection as well.

One ethical and compliant way to gather additional user data is through gamification. By integrating quizzes or interactive elements, users can voluntarily provide data in a fun, engaging manner (Fryman, 2021). This not only enhances the user experience but also ensures that data is collected transparently and consensually.

We must also reduce the scope of data collection to fit within data minimization and purpose limitation guidelines by only collecting the data that fits our goals and nothing more. We simply need to streamline our data collection to fit our needs, which should lead to minimal impact on the user’s end.

The proper use of encryption will aid in establishing a robust system that will protect data at rest and in-transit. This will help us fit within the GDPR’s expectations defined by the accountability principle which expects the business to implement the necessary and appropriate measures to protect user data and be able to ensure they follow the law. (European Data Protection Supervisor, n.d.)

Differential privacy (DP) is another recommended approach to safeguard user data. By adding random noise to data points, DP protects individual privacy while still allowing for useful data analysis. This method ensures that no individual’s personal data is easily identifiable while enabling us to analyze patterns and improve the user experience. (Dorschel, 2019)

While neural networks play a major role in enhancing the user experience and aiding in business revenue, ensuring compliance with the GDPR is required to remain ethical and avoid legal issues. Through the methods of transparent data collection, limited data use, and a focus on privacy preservation through techniques such as encryption and differential privacy, we can proceed under legal compliance and build trust with our user base.

# References

Denison, G. (2023, October 24). *4 shocking AI bias examples*. Retrieved from Prolific: https://www.prolific.com/resources/shocking-ai-bias

Dorschel, A. (2019, April 24). *Rethinking Data Privacy: The Impact of Machine Learning*. Retrieved from Medium: https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

European Data Protection Supervisor. (n.d.). *Accountability*. Retrieved from European Data Protection Supervisor: https://www.edps.europa.eu/data-protection/our-work/subjects/accountability\_en

Fryman, O. (2021, April 18). *Personalization in the Age of GDPR*. Retrieved from Syte: https://www.syte.ai/blog/personalization/personalization-in-the-age-of-gdpr/

New York Institute of Technology. (2023, December 12). *Neural Networks 101: Understanding the Basics of This Key AI Technology*. Retrieved from New York Institute of Technology: https://online.nyit.edu/blog/neural-networks-101-understanding-the-basics-of-key-ai-technology

Richard, J. (2023, June 19). *Balancing Users’ Data Privacy and the User Experience*. Retrieved from UXmatters: https://www.uxmatters.com/mt/archives/2023/06/balancing-users-data-privacy-and-the-user-experience.php

Spillane, J. (2022, December 08). *How GDPR Can Undermine Personalization and User Experience*. Retrieved from Business2Community: https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

Ved, A. (2019, Febraury 28). *TechGDPR*. Retrieved from How to develop Artificial Intelligence that is GDPR-friendly: https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/

Yasar, K. (2023, March). *black box AI*. Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/black-box-AI