In today’s digital age, personalization has become the cornerstone of end-user experiences, particularly regarding social networking platforms that have a reliance on advanced technologies. One such technology is neural networks, a form of machine learning (ML) algorithm that attempts to mimic the workings of a human brain & anticipate its user needs & preferences. However, as the European Union’s General Data Protection Regulations (GDPR) constantly update & shape the global landscape of data privacy, all companies must make sure their practices remain in line with the standards. I am writing this white paper to address concerns raised by an EU regulator with regards to potential GDPR violations stemming from our company’s use of neural networks regarding personalization. By explaining how neural networks function, evaluate their ethical implications, analyze GDPR principles affecting our practices, assess legal concerns, and propose actionable adaptations, this paper can be put forth as a guide for our team to adhere to compliance & keep its competitive edge.

Neural networks are computational models that consist of layers of interconnected nodes, referred to as neurons, that mimic the structure & function of the human brain. These can be further categorized into three layers.

* ***Input Layer*** – Receives raw data inputs
* ***Hidden Layer*** – Processes the inputs through weighted connections & applies activation functions to capture complex patterns.
* ***Output Layer*** – Tasked with producing the result, such as classification into split categories.

When we used ML for personalization, the neural networks analyze user data, such as the clicks, path of navigation, & time spent on an item or in a group, to identify patterns while predicting the user’s next action. These methods allow us to tailor the end user experience. The primary strength of a neural network is the ability to learn & adapt as time goes on. When initially training the network, the weights are adjusted to minimize errors, enabling it to make increasingly accurate predictions as time goes on. While this is an effective process, it raises flags for the transparency & data usage. Our algorithm’s way of delivering ads based upon this learning & increasing click through rates, is the cause of the potential violation. Some recent examples also express concern for bias in the algorithm, which stems from different data training techniques that could lead to discriminatory outcomes. If a certain selection of data is overrepresented based on demographics, our algorithm my show favor to a select group, which promotes inequality.

The GDPR has outlined several principles that pertain to our practices. We need to be more open & transparent when explaining to our users about our data collection methods & what we do with their information. By adhering to principles below, we have direct impact on our company’s use of neural networks for personalization.

1. ***Transparency*** – Require us to inform users about how their data is being collected, processed, and used. To be complying, we must provide clear, user-friendly explanations of our algorithms and data practices.
2. ***Purpose Limitation***- Require our company to stipulate that data can only be collected for a very specific purpose with predetermined limitations and will not be repurposed without user’s consent. This will also impose limitation on the archiving & reusability aspect of user data for future applications.
3. ***Data Minimization***- This principle should be looked at as a mandate to reinforce that data will only be collected for its stated purpose. This should reduce the risk of data breaches but may potentially slowdown the performance of our neural networks.
4. ***Accuracy***- Requirements to keep up-to-date records, & update as needed. This means ensuring that user profiles reflect current preferences & behaviors.
5. ***Storage Limitation***- This principle places a limitation on the indefinite retention of data. By implementing policies to delete outdated or irrelevant data, shouldering the compliance load while keeping a robust & growing training database.
6. ***Confidentiality***- This principle emphasizes the importance of securing user data against unauthorized access or potential security breaches. Improving our security with robust encryption, access controls, & regular audits to help manage any potential leaks.
7. ***Accountability***- Keep the company held accountable to the highest standard by demonstrating compliance with GDPR principles. Maintain detailed records of data processing & conduct regular assessments to self-identify & mitigate risks.

GDPR’s requirements pose significant legal & operational challenges for our company. Non-compliance could result in hefty fines, reputational damage, and loss of user trust. However, abandoning data collection is not a viable option, as personalization is central to our business model. Our main business model stems from targeted advertising, based on the data we collect & allows us to stay ahead of our competition. Instead of eliminating the data collection, focusing on adopting new responsible practices aligning with GDPR will help us in the current day & future. Making sure to not collect excessive amounts of data which may not be useable outside our scope of data training would be a great start.

Enhancing transparency, clear implementation, accessible privacy notices with breakdowns detailing the data collection & processing activity. Our industry has also adopted the “right to be forgotten”, which allows users to control how their data is being used, especially personal identifiable information. Users can submit without a click an option to request their data be deleted, no needless hoops or links & guidelines to follow, simplify the process to remain complaint. Making sure that all data remains heavily encrypted to protect its sensitive nature & limit access is another step. Data removable once no longer in use also needs to be implemented, as to avoid future archiving and adhering to storage limitation principles. By regularly assessing and mitigating biases in neural network models will ensure fairness & compliance.

In conclusion, the GDPR presents both a challenge & an opportunity for our company. While its principles impose strict requirements on data usage, they also set the precedent our company needs to follow for compliance. y understanding the basics of neural networks, addressing ethical concerns, and adapting our practices to comply with GDPR, we can continue to deliver personalized user experiences while safeguarding user privacy. Ensuring the quality of our user experiences allows for trusts from the consumer, legal compliance, & ethical standards in data processing.

Spillane, J. (2022, December 8*). How GDPR can undermine personalization and user experience*. Business 2 Community. https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

Gulli, A., & Pal, S. (2017). Deep learning with keras : Get to grips with the basics of Keras to implement fast and efficient deep-learning models. Packt Publishing, Limited.

Najibi, A. (2020). *Racial discrimination in face recognition technology*. Science in the News. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology

Moore, M. (2024, March 25). *Understanding AI vs. Neural Networks*. Shakuro. https://shakuro.com/blog/ai-vs-neural-networks

*AI vs. Machine Learning vs. Deep Learning vs. neural networks*. IBM. (2024, November 25). <https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>

Silipo, R. (2020, March 3). *How to keep bias out of your AI models | CustomerThink*. Customerthink.com. <https://customerthink.com/how-to-keep-bias-out-of-your-ai-models/>

Janet. (2021, January 15). *Overcome and Prevent Bias in AI - Figure Eight Federal*. Figure Eight Federal. <https://web.archive.org/web/20240710160510/https://f8federal.com/overcome-and-prevent-ai-bias/>

Heilweil, R. (2020, February 18). *Why algorithms can be racist and sexist*. Vox. <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency>