GDPR Compliance for Personalization with AI Neural Network

### Shawn Millin

### CS-370

### Septmeber 28th 2025

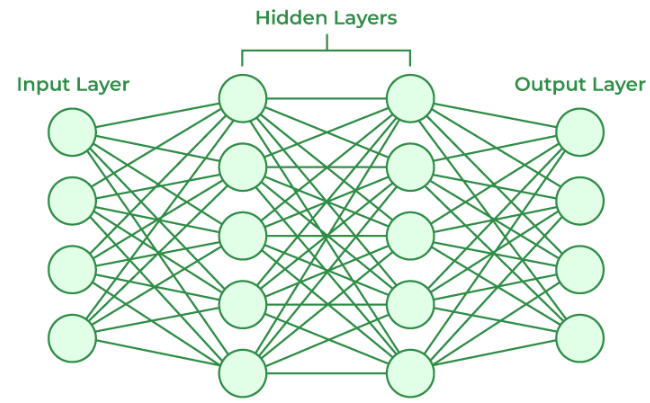
## Abstract:

It has come to our company’s attention that GDPR laws or regulations may be in violation due to our gathering of data for personalization of a user’s experience on our website. A brief background of the AI neural network used for personalization is presented here. Findings from the GDPR are presented in response to possible violations as well as solutions to the possible violations.

## Artificial Neural Network:

The Artificial Neural Network is a human made computing system which is intended to mimic the neural system of the human brain for the purpose of analyzing data, identifying patterns, and to make predictions. This system is a simplified version of the actual human neural system consisting of artificial neurons in three layers to form it’s framework: the input layer, the hidden layer, and the output layer.

The Artificial Neural Network visual:

 GeeksforGeeks (2025)

Each circle above is a neuron in the network with the lines showing that each neuron is connected to each of the neurons in the following layer of neurons, each connection given a value called weights, with data traveling from the input layer through to the output layer. The input layer is the receiving part of the network where information is entered such as an image, the hidden layer is the processing part of the network where hundreds to thousands of neurons connect to learn and understand, and the output layer is the decision or prediction layer. There are different types of neural networks based on the algorithms used such as Convolutional Neural Networks (CNNs) for image data and Recurrent Neural Networks (RNNs) for sequential data. The process of learning in a neural network starts with training the network in that it is shown hundreds to thousands of images or text of the object a developer wants the system to predict. The developer then assigns weights, values, to the neuron connections and begins testing the network’s ability to predict the object. “Training ends up finding the appropriate weights and biases, utilizing the backpropagation algorithm, which calculates the derivative of each layer's function after every pass of the data through the network, in order to determine the changes that need to be made to the network's weights.” Science Direct (2022). The backpropagation mentioned computes gradients of the loss function, error calculation, by working from the output layer backward to the input layer. Several passes of the data through the network are made in order to find a better fit to predict the input data correctly.

## Neural Networks for Personalization:

The AI neural networks are used by companies to personalize a user’s experience on the company’s website by predicting preferences and behavior. By using this technology a company can recommend certain items, price ranges, and tailor content for each user. This is accomplished by gathering the users’ data from browsing history, purchasing patterns, product ratings/reviews, and demographic information. After data collection a company prepares the data for training, “This step involves cleaning the data, handling missing values, normalizing numerical features, and encoding categorical variables.” The Economic Times(2023). The neural network is designed with the appropriate model such as CNN or RNN then trained with the prepared data. The training allows the network to learn the patterns and relationships in the data and adjusted to minimize the prediction errors. The predictions of the users’ data is used to generate recommended items in a ranked list.

With this use of an AI neural network to personalize a users experience some ethical issues become evident and may force a company to adjust their technology to comply to laws and policies. Two such ethical concerns are: who is deciding where the line is of being helpful ends and when is the line is crossed into manipulating or targeting users, as well as privacy and consent concerns. When companies go too far in collecting customer data they end up loosing customer trust, “According to a 2023 Pew Research survey, 79% of Americans are concerned about how companies use their data.” and “A 2022 study by Accenture found that 41% of consumers find it "creepy" when brands know too much about them.” Brooker(2025). Many times customers feel this way because they were never given the option to opt-out of personalization from data collecting which violates their consent. Manipulation and targeting are a problem when personalization is too rigid or specific, this becomes turns the predictive outcomes of a neural network unhelpful such as when a customer is looking for a helpful solution but is instead bombarded with ads to by products. The overly specific out comes of neural networks, called over-fitting, is also harmful to customer-experience because it allows segregation from diverse content.

Some companies choose to use “black-box” AI to perform data collection and decision making for efficiency. “Black box AI is any artificial intelligence system whose inputs and operations aren't visible to the user or another interested party.” Awati(2024). The use of “black -box” AI machine learning is problematic for both customers and the developers because customers are unknowingly being monitored violating privacy rights and developers do not know how the system is arriving at its conclusions so they are unable to correct or update the system.

## GDPR affecting personalization:

There are regulations that protect the public from unlawful data collection. The General Data Protection Regulation (GDPR) is a European law which sets strict rule for how companies collect, use, and protect the personal data of people living in the European Economic Area (EEA). These regulations directly affect the data collection process for personalization. Transparency in the GDPR comes in the form of the “right to be informed” and “Subject Access Requests” where people have the right to have access and be informed about their personal data that is collected and companies must comply and respond within one month. “The information you [the company] provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.”ico(2025). The GDPR has a principle for data minimization for companies to follow in that the processing of personal data must be ‘necessary’ for a specific purpose but if this specific purpose can be achieved with out the processing there is no lawful basis for processing the personal data. The accuracy principle in the GDPR states, “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.”ico(2025). The GDPR also has a principle for storage limitations which states, “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.”ico(2025).

## Company practices affected by GDPR:

In reviewing the GDPR guidelines, laws, and regulation there are a few areas that our company will need to make adjustments in to follow these laws. There is a possibility of manipulation from maximizing the time spent on the site and maximizing the number of ads the user clicks on. Mouse clicks in general can be intrusive by gaining data on a user’s behavior, emotional state, or health condition violating their consent. Possible storage limitation violation by feeding data through multiple neural networks with no mention of a plan to deletion no relevant data or data that has already been used for its intended purpose. Our company has no mention of the option for customers to opt-in or opt-out of data collecting processes nor information provided to customers on whee they can access the data gathered. Excessive targeted advertising could be seen as a consent violation as the user did not authorize the company to send them advertisements. Knowing everything there is to know about a user is a data minimization violation because not all information is ‘necessary’. Location data may not be ‘necessary’ for all personalization neural networks as well. It may be possible to not collect data via the current algorithmic methods in favor of alternative first-hand voluntary methods such as customer feed back and surveys on what the user wants to see in their experience except the user click information is no possible to be obtained outside of counting the clicks. Contextual data can be used, “personalization can be based on non-private data, such as: the time of day, a user’s general geographic location(city or state), the device they are using.”Daniels(2024).

## Adaptations:

In response to the findings of possible violations against the GDPR our company is ready to discuss the changes necessary in order to be compliant with the GDPR. The company will focus on the key principles of the GDPR of Transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Confidentiality, and Accountability. Transparency will be adjusted to include permissions from users to opt-in or opt-out of data gathering and what the data is used for with literature on how to access the gathered data for the individual user’s information, as well as using “white-box” AI to understand the decisions made by the neural network. To comply with purpose limitation, storage limitations and accuracy, our company will design an audit that will be conducted on data processing activities to identify any unintended uses, data stored longer than needed, and inaccurate data. Data minimization will be in the form of minimizing the amount of personal information scrapped from the company’s websites and integrating first-hand data gathering of voluntary information for more ‘necessary’ data. Confidentiality and accountability will be shown in the form of not sharing data with unauthorized users or third-parties and implement strong security measures such as encryption.

Resources:

GeeksforGeeks. (2025). *Artificial Neural Networks and its Applications.*<https://www.geeksforgeeks.org/artificial-intelligence/artificial-neural-networks-and-its-applications/>

Science Direct. (2022). *Neural networks and backpropagation.* <https://www.sciencedirect.com/topics/computer-science/neural-network-training>

The Economic Times.(2023). *How deep learning works and how it’s used to create personalised recommendations.* <https://economictimes.indiatimes.com/news/how-to/how-deep-learning-works-and-how-its-used-to-create-personalised-recommendations/articleshow/101689849.cms>

Brooker, Michael. (2025). *AI and the Ethics of Personalization: finding the right balance.* Busy seed. [https://www.busyseed.com/ai-and-the-ethics-of-personalization-finding-the-right-balance#:~:text=Without%20transparent%20policies%2C%20businesses%20risk,echo%20chambers%20that%20reinforce%20biases](https://www.busyseed.com/ai-and-the-ethics-of-personalization-finding-the-right-balance" \l ":~:text=Without transparent policies%2C businesses risk,echo chambers that reinforce biases).

Awati, Rahul. (2024). *What is black box AI?*. Tech Target. <https://www.techtarget.com/whatis/definition/black-box-AI>

Spillane, James.(2022). *How GDPR Can Undermine Personalization and User Experience.*Business2Community. <https://web.archive.org/web/20230330083650/https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269>

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

Ved, Anamike. (2019). *How to develop Artificial Intelligence that is GDPR-friendly.* Tech GDPR. <https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/>

Hanaia, Pierre-Andrien. (2018). *AI and the Janus face of the GDPR- chance or challenge.* Capgemini.<https://web.archive.org/web/20210116193317/https://www.capgemini.com/2018/11/ai-and-the-janus-face-of-the-gdpr-chance-or-challenge/>

ico. (2025). *UK GDPR guidance and resources.* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

Daniels, Jodi. (2024).*How to Provide Customers Personalization Without Data Privacy Invasion.* Red Clover.[https://redcloveradvisors.com/how-to-provide-customers-personalization-without-data-privacy-invasion/#:~:text=1.,of%20first%2Dparty%20data%20programs](https://redcloveradvisors.com/how-to-provide-customers-personalization-without-data-privacy-invasion/" \l ":~:text=1.,of first-party data programs).