Date: September 27, 2025

Author: Rolesshania- Lead Engineer, Personalized Algorithms

Audience: Systems Engineers, Software Developers, AI Experts, Legal Team

Company’s success in delivering hyper- personalized user experiences is driven by neural networks that analyze behavioral data to recommend data to recommend content, connections, and advertisements. However, data-centric model has raised concerns from EU regulators regarding compliance with GDPR (General Data Protection Regulation). In further explanation, this will highlight how neural networks function, evaluate their role in personalization, and propose a step-by- step to align out practices with GDPR principles while preserving user engagement and business viability.

Neural networks are computational models inspired by the human brain. This consists of three main layers:

* Input Layer (location, time on page) receives raw data
* Output Layer (“Suggest this friend”) produces predictions or classifications
* Hidden Layers- perform complex transformations using weighted connections and activation functions. Layers detect patterns and relationships in the data.

Furthermore, each neuron will pass through its output to the next layer, and the network adjusts its internal weights during training to improve accuracy. This process can help the system to classify user behavior and predict preferences with high precision. With neural networks power our personalization engine by:

* analyzing user behavior to recommend posts, friends, groups and ads
* Learning from past data to anticipate future interests/movements
* Continuously refining predictions as new data is collected

“Block Box” classification means the system makes decisions (such as recommendations of a post or predicting a user (customer) interest) but can’t easily see or understand how it reached that decision.

***Example: If you gave the system some data (time spend on a page such as Dog Lovers), and it gives you a result like, “You might like this Instagram page for Las Vegas Dog & Coffee Group.” But if you ask, “Why did it recommend that?”, the answer won’t be clear.***

Ethically, the “Black Box” raised concerns for:

* Hidden Biase- models may reinforce stereotypes or exclude minority groups if trained on biased data
* Lack of Transparency- users (customers) cannot see or understand how decisions are made
* Autonomy Risk- over personalization may limit user exposure to diverse content, creating echo chambers.

GDPR Principle Impacting Personalization:

Transparency

Users have the right to know HOW their data is being used. If our system recommends a post or ad, we need to clearly EXPLAIN what data was used and why. This builds trust and helps users feel in control of their experience.

Confidentiality

User data must be protected from leaks, hacks, or misuse. That means using strong security tools like encryption and limiting who can access sensitive information. If we collect personal behavior data, we have to keep it safe.

Accountability

We’re responsible for how we use data. If something goes wrong (e.g. privacy breaches) we need to show that we follow the rules and execute procedures step by step to prevent them. This will mean keeping records, reviewing our models, and assigning clear roles for oversight.

Purpose/Storage Limitation

We can only collect data for specific reasons, like improving recommendations or targeting ads. We can’t reuse that data for unrelated features unless users agree. Also, we shouldn’t keep data forever, as long as it’s needed for its original purpose.

Legal Concerns

In regard to legal concerns that may arise from our companies, profiling and automated decision-making. GDPR Article 22 restricts decisions made solely by automated systems that significantly affect users. And also consent validation, making sure that consumers’ consent must be informed, specific, and revocable. When collecting data, our companies best defense relies on behavioral data to deliver relevant information/content and ads. Without data collection, personalization, and monetization, this would cause a collapse. There are alternatives like contextual advertising lack precision and reduce click- through rates.

Not collecting data is NOT VIABLE option for the company’s business model, especially given its reliance on neural networks for personalization and targeted advertising. Neural networks require a significant amount of user data (e.g. clicks, time spent on pages or even navigation patterns) to learn and predict what content, friends, or ads a consumer might engage with. Without this behavioral data, the system cannot personalize their experiences. This is central to consumer satisfaction and retention. Overall, the company’s model is built on high click- through rates from personalized ads. If you are not aware, Ads are very effective because they are personalized to the consumers interests, which increase from user data. Without data, ad targeting becomes boring, reduces engagement and revenue. The balance of legal and ethical ways, while GDPR demands strict controls, does not prohibit collection of data. This requires complete transparency, consent, and purpose limitation. This solidifies the importance of asking for clear, informed consent, minimizing unnecessary data collection, and providing explanation how data is used. In all actual perspectives, data collection is essential to the company’s personalization and monetization strategy. You would think the easiest solution is to stop collecting, but to collect responsibly, transparently, and within compliance with GDPR.

Reference:

GDPR Advisor. (2025). *How GDPR affects AI-powered personalization in digital marketing.* GDPR Advisor. <https://www.gdpr-advisor.com/how-gdpr-affects-ai-powered-personalization-in-digital-marketing/>

GDPR-info.eu (2025). *Art.22 GDPR- Automated individual decision- making, including profiling.* [*https://gdpr-info.eu/art-22-gdpr/*](https://gdpr-info.eu/art-22-gdpr/)

TechGDPR. (2022, October 18). *How to develop artificial intelligence (AI) that is GDPR-friendly*.<https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/>