Lawrence Artl III
CS 370 22EW1
Project One
September 19, 2022

# Bringing Our Company into Compliance with the GDPR

Artificial Intelligence has been around for some time now, but only recently (within the past ten or so years) has it become so mainstream in its usage. Once the stuff of “science fiction”, Artificial Intelligence (henceforth referred to as AI) is now used in so many industries it’s hard to imagine what the world was like before its intoduction. Our company is no different from many other social media giants in that we too employ AI in order to better serve our customers and users. Personalizing an experience for all of our users is an undertaking fit only for a computer with a brain like no other, powered by AI to predict the most relevant content that a user will engage with and serve it up as quickly as it can be generated. Our platform does this amazingly well, and our click-through rate is double that of our closest competitor thanks to the algorithms used.

In order to ensure that every user gets the experience they will engage with the most, our company collects a large amount of data on them. This data is used to “feed” the algorithms that power the AI in charge of predicting the most relevant content to show. The data points collected include things like mouse clicks, site navigation maps, time spent on pages location data, and so on. Essentially, everything a user does with the application environment is saved and fed into the algorithms. This unfortunately has left the company in a position where it potentially violates some terms of the General Data Protection Regulation, or GDPR. An EU regulator has recently brought this to the company’s attention, voicing their concern about whether our business model conforms to some of the principles defined by the law. Needless to say, this is of utmost importance and should be addressed immediately to avoid litigation or other such legal procedures.

In this report we will start by exploring several items, starting with what the company's AI does and how it works, as well as how we use it to create personalization for our users. We will also further define the GDPR, specifically the aspects that have been isolated as potential areas of violation. How the GDPR is affecting our company-wide practices will also be addressed. We will then propose ways to address the concerns that have been brought forth by the regulator, as well as possible changes to the company's business model that will further ensure our compliance with the GDPR for the future.

## How does AI work?

Artificial Intelligence is made possible by something called a "neural net", which is exactly what it sounds like: a network of "neurons" that are all linked together and working in tandem to solve problems. The neural net in computers works very similarly to the neural net of the human brain. Neurons are networked together and information is passed between them; connections are made stronger by repeated associations of information, and these strong connections are then used to make predictions about future data points. In the case of a computer neural network, the neurons are not cells but instead mathematical equations, algorithms that take inputs of data, perform calculations on them, and return outputs of that data (Shin, 2020).

At its core, a basic neural network consists of layers of neurons that are interconnected together and allow data to flow from input to output. As the data travels from one layer to the next it is passed to neurons that either become activated or not. The activation of a neuron by the data creates an association, which then strengthens the connection between the two. The more these two neurons activate together, the stronger the connection and thus the stronger the association. As an example, if a certain type of data always activates the same neuron set that another type of data activates, the network will learn that these two pieces of data are related in

some way, and thus predictions can be made about one or the other when new similar data is encountered.

How does all this relate to personalized experiences for our users? Every user of an application produces data of some sort. This data can be used to predict the behavior of a user and ultimately tailor an experience for the user based on these predictions. The data that is collected is fed into the company's neural network, which passes the data through the layers, activating different neurons along the way and building associations. The more data that is fed into the network, the better the network becomes at predicting connections between other data points.

Consider a user who enjoys running in marathons. If every time a local marathon is announced this user searches within the application for running shoes to purchase, the neural network can build an association for the user based on these two data points: marathons and new shoes. Thus, if the network becomes aware that a new marathon has been announced for the location in which the user resides, advertisements and relevant articles about the latest running shoes and running shoe technology can be pushed to that user before they even start searching. Likewise, if the user is found to be searching for running shoes on their own, the network can search for and reveal future marathons that may interest the user, since these two data points are associated with one another.

This same scenario can be applied to countless other types of data associations: local dust storms and cleaning supplies, new pets and pet-care items, or house-hunting and local schools.

### Is this an ethical practice?

The ethics of this practice are always questioned, and to be truthful it is a somewhat "gray-area" of ethics overall. While users are informed when creating an account that their data will be collected for personalization of their application environment, the algorithms within the

neural net or how Artificial Intelligence makes its predictions based on the data collected is not made known. In fact, most developers of the software that powers the neural net and AI don't even know how the algorithms work! This "black box" scenario does raise some questions about whether the data is being used correctly, anonymously, or even fairly.

As a general point, depending on the purpose of a neural network and the data collected, users of an application may get a personalized experience that isn't necessarily what they expected, but instead works to shape their thought process and future decisions. Does this scenario apply to our company? Currently it is not known.

### What exactly is the problem, then?

This issue with using these technologies is that neural networks lack context, and therefore only make associations and predictions about data as a machine would, lacking understanding of the data itself. The network's algorithms may find associations that a human interpreter may never consider, and the network may even have bias written in where there was never meant to be a bias (Cockrell, 2019). The network could potentially push content to users that may seem harmless at first, but slowly move their interactions towards an extreme that ultimately shapes the way the user thinks. Because so much content exists, the network must narrow the scope down to a small percentage of related content to show the user. This content will typically be of types that elicit the most responses from a user, keeping them engaged in the application (Shapiro et al., 2022).

As an example, a user could select an article that contains some misinformation about a particular topic that they are interested in. As innocuous as that action may seem, the network could use this as a template for future articles to show the user about the same topic. Content that the user sees could more often contain increasing amounts of misinformation about the topic they want to read about, causing them to continue to read the misinforming articles and

thus remain engaged. The neural network does not understand that the articles it is pushing are full of false narratives; it only associates user interaction with these types of articles.

Unintentional biases may exist within the network as well, due to no fault of anyone but simply created through simple machine learning. Users who frequently misspell words or use incorrect grammar in their posts could be flagged by the network as being less educated than users who do not misspell or use bad grammar, and this could lead to hidden biases emerging in the content they see more often. With a network assuming that a frequent misspeller is less educated, that user may see content that is less thought provoking, lower in scientific standards, fraught with inaccuracies, or prone to other such errors that higher-level users would not interact with. While it ultimately is the user's decision to interact with the content they are provided with, when walled into an application that minimizes the type of content a user sees, one can imagine the beginnings of an echo-chamber forming for these users. Essentially, if the only related content a user gets is of a certain calibur, then he or she may begin to think that that content is the only content that exists for the topic in question.

### What is the General Data Protection Regulation?

Implemented in the EU in May of 2018, the GDPR serves to protect user privacy when data collection is a component of a business that said user interacts with. While the GDPR is most commonly associated with online privacy, it can be applied to all data collection scenarios. The GDPR allows provisions for the regulation of how personal data is collected by an entity and how that data is used. By design, the GDPR lists very strict principles to protect the rights of any user or "data subject".

In relation to a user's privacy there are several principles of the GDPR that affect the personalization of an application like the one that our company has developed. These principles are defined as follows.

- Transparency: The use of personal data by an entity must be disclosed to users in a clear, open, and honest way from the start. Data usage must be transparent to users in a way that allows them to make the right decision about whether to allow their data to be used in such a way. Many users will lack technical knowledge, so it is the entity's responsibility to use clear and plain language when explaining how a user's data will be used.
- Purpose Limitation: As with transparency, an entity must also disclose in a clear and concise manner the purpose for processing a user's data. Data should only be collected for specific (explicit) purposes; the data should not be used for further purposes that are not disclosed to the user. If personal data is collected from users to further the user's experience in an application per the disclosed purpose, then it would be a violation to then sell said data to a third party without disclosing it to the user beforehand and offering a chance to opt-out.
- Data Minimization: Data minimization is linked to purpose limitation in that only the necessary user data to fulfill the stated purpose should be collected from the user. Any data that is collected need be relevant to the completion of the stated purpose as well, meaning extraneous data that does not fit with the stated purpose should not be collected. For example, if an application uses location data to recommend restaurants to eat at, a user's PII (Personally Identifiable Information) beyond their location is likely unnecessary to collect and therefore should be ignored.
- Accuracy: Data collected from users should be as accurate as possible given the circumstances and limitations of technology. Every effort to correct incorrect data should be taken (within reason) in order to ensure all data collected on an individual remains up to date. Ensuring data accuracy ensures the user not only gets the most personalized experience, but also maintains security and privacy for other individuals.

- Storage Limitation: Any personal data that is collected from a user should not be kept longer than it is needed. The length of time will be dependent on the purpose that the given entity intends to use the data for. Some applications may keep personal data indefinitely if it serves a greater purpose, like serving customers relevant content or maintaining a current address for shipping. If data is no longer needed, an entity should consider erasing it; if the user returns and the data is no longer available, procedures would be in place to reinstate the data one way or another. Users may forget that they have their personal data stored in any number of accounts nowadays, and keeping extraneous data could open an entity up for security issues if there are data breaches.
- Confidentiality: Appropriate security measures must be in place to protect all users' personal data that is held by an entity. All processing must exist in secure environments, and any data that is stored must also be secured by highest industry standards.
- Accountability: An entity is responsible for what is done with user's personal data and appropriate measures and records must be in place to demonstrate compliance. This includes implementing security measures and data protection policies.

All of the above principles are written to protect the privacy of users and their data. What this ultimately means, though, is that entities like ours must abide by these principles very closely, lest we be the subject of litigation for violation of the GDPR.

## How does the GDPR affect our company practices?

By and large the most pressing issue to deal with here is the data minimization principle in the GDPR. This principle states that entities must limit their data collection only to what is necessary in order to fulfill a purpose (*Guide to the UK General Data Protection Regulation (UK GDPR)*, n.d.). However, with such a broad purpose as "personalized user experience" it is hard to determine if all data collected does in fact align with this business goal. The user definition of

a personalized experience may differ from the company's, resulting in the user getting an experience that is less about serving them content they desire and more about serving content that the business feels will keep them engaged with the application the most.

This also brings to consideration compliance with purpose limitation and data collection. With a broad purpose of enhancing the user experience on the application, collecting all manner of data from users could potentially fit towards this goal, yet at the same time be completely irrelevant overall. Using the grammar and sentence structure of a user's posts to build a profile about their level of education would likely be considered an overreach by most users. Serving content that contains misinformation to users based on their interaction history could also be problematic, as this could shape the way a user thinks in a way that they may not consent to if they were aware of the process. While these two scenarios would both arise from biases that were not intentionally written into the algorithms powering the AI, intent is irrelevant when the law is concerned. We as a company are responsible for how the data is used, regardless if we intended to use it that way or not.

Depending on the structure of the algorithms involved in the neural network designed to learn about users' activities and push relevant content, users may get an experience that does not align with the transparency principle of the GDPR. Being transparent requires an entity to disclose in a concise and tech-friendly manner the way in which user's data is being harvested and subsequently used (*Guide to the UK General Data Protection Regulation (UK GDPR)*, n.d.). However if the algorithms are either unknown, undisclosed, or simply too complex for users to understand, then it could be written off by many as simply some sort of "behind the scenes magic" that compiles user activity and predicts content matches for them. Users should be fully aware of not just how their data is being used but how it is collected and processed, too. A perceived lack of transparency in this regard could make the company vulnerable to litigation should users feel they were misled about how their data was being harvested and for what purposes.

## Can we as a company just stop collecting user data?

While this is a potential route to take in order to ensure complete and total compliance with the GDPR, it is unfortunately not possible. With a business model driven by user interactions and click-throughs on the application, the company cannot afford to simply not collect any data about users at all. Users are more likely to interact with an application that offers a personalized service (*Personalization Pulse Check*, 2018), and since our application revolves around user interaction, this is an important feature to include.

However, not all currently collected data is necessary to serve this personalized user experience. There will be certain data points used in order to best serve them the content they desire. This data may include post interactions and any “following” lists. Data that could potentially lead to unexpected biases (like racial or ethnic backgrounds, socioeconomic standings, marital status, etc) should not be collected, even if the users include them in their profile or posts. Allowing users to complete an “interests” questionnaire when first creating an account, and allowing them to update this as they use the application has the potential to allow for maximum transparency and user control over what data they share. The algorithm can use this information to predict what similar or related content the user may also like to see, but the majority of content will be based on the interests list that they control.

It may not be fully understood just what some data points will result in when fed through a black-box algorithm. As mentioned previously some data that could be collected and processed may result in less than ideal content being served to users. Unbeknownst to these users their own data could be used to govern their own feelings, opinions, and overall view of the world. This is cause of concern on an ethical level, but more so opens the company up to potential liabilities should users become aware of this. Additionally, while users may never fully understand or be aware of how the company algorithms determine the content they see, freedom of interaction should always be a top priority with any content serving company.

Allowing users more freedom to discover content that they wish to interact with is preferable to force-feeding them content that the company thinks they will interact with more. While this may prove to be a slightly-less profitable business model, the overall benefits to both the user base and the company will potentially outweigh any “losses” that may be incurred. These benefits include a happier user base, more stimulating content, and investors being protected from negative press or reviews.

### How can the company adapt its practices to comply with the GDPR?

Aside from some of the suggestions listed in the previous section, there are some standard practices that many similar companies have adopted in order to maintain full compliance with the GDPR. These adoptions will take time and manpower to implement fully, but they will also limit the company’s liability in regards to data collected from the users.

- Using good data hygiene - only using necessary data types to create an AI are collected from users (Medairy, 2020). Keeping this data secure is top priority, and only kept for as long as necessary to accomplish the purpose of the system. This relates to storage limitations in the GDPR. Once data is no longer needed it should be scrubbed from all hard drives or servers in a way that makes it irrecoverable by anyone.
- Using good data sets - fair, accurate, and appropriately representative datasets should be used when building an AI. Using AI algorithms to audit the quality of other algorithms should be done where possible (Medairy, 2020). This practice will ensure that users’ data is representing them correctly and fairly with minimal bias towards any group or groups. Data that is used to determine a unique user profile should be free of any bias before being used to train AI algorithms. As mentioned above, allowing users to build the personalized data list that will be used to develop their personalized experience will give them complete control and will help to minimize biases generated from machine learning in the algorithms.

- Giving users control of the data they share - not only should users know what data is being collected and shared, but they should have the option to modify what data is shared and completely opt out if they wish (Medairy, 2020). Users should be expressly informed, in plainest terms possible, how their collected data will be used to train the AI and what the AI algorithms are expected to serve them in return. Likewise, users should have the option to be completely forgotten should they choose to leave the application and delete their profile; this will ensure their data is never used again (Spillane, 2018).
- Ensuring data is inclusive - the data that is used to train AI algorithms needs to be inclusive of all groups, even those that make up a small percentage of the general population (Medairy, 2020). This will help to create a broad and more representative profile of the demographic being served.

Considering the above best practices, there are several things the company can do in order to change the way data is collected, stored, and used to build personalized experiences in the application. First and most importantly, users need to be informed of exactly what data is being collected and how it is being used. This will ensure transparency of how the business serves the users content through artificial intelligence. Users must have the option to not share any data at all, or restrict certain data points from being tracked by the company, and they must be informed as to how this will affect their experience within the application's environment.

Next, any user data that is collected must be properly anonymized before being fed into any AI algorithms to maintain privacy. This includes stripping usernames and other personal data, normalizing times of events, and generalizing location data to large regions as opposed to more accurate results.

Once the data is collected and processed, everything possible should be done to remove the data in a way that makes recovering it again next to impossible. Removing used

data will keep the company in compliance with the GDPR's "storage limitation" principle, as well as aid in ensuring data security and data anonymity.

Finally, every measure necessary to remove bias from the AI algorithms should be implemented at once. Bias towards race, gender, language spoken or read, able-bodiedness, intellect or education level, socioeconomic status, and religion should be removed. Additionally the datasets that are fed to the algorithms for training should be representative of the entire population of expected users, with no one subset being favored in the data over any other.

With these implementations, the company can move towards being fully compliant with the GDPR, but more so we will be serving out users better. Ensuring data privacy is everyone's responsibility, but we as a company that collects data from users have been trusted to do the best we can with that data. Moreover, ensuring that our user's data is used properly by our algorithms and Artificial Intelligence should be of utmost importance. Complying with the principles of the GDPR can help us to reach the goal of a personalized user experience while using the minimum amount of data necessary to do so.

## References


Cockrell, J. (2019, May 28). *A.I. Is Only Human*. Chicago Booth. Retrieved September 19, 2022, from https://www.chicagobooth.edu/review/ai-only-human

Dorschel, A. (2019, April 25). *Luminovo Blog | Data Privacy in Machine Learning*. Luminovo. Retrieved September 14, 2022, from https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

*Guide to the UK General Data Protection Regulation (UK GDPR)*. (n.d.). ICO. Retrieved September 14, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Isaak, J., & Hanna, M. J. (2018, August). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *The Policy Corner*. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400

Medairy, B. (2020, January). *4 Ways to Preserve Privacy in Artificial Intelligence*. Booz Allen. Retrieved September 14, 2022, from https://www.boozallen.com/s/solution/four-ways-to-preserve-privacy-in-ai.html

*Personalization Pulse Check*. (2018). Accenture. Retrieved September 19, 2022, from https://www.accenture.com/t20161011T222718__w__/us-en/_acnmedia/PDF-34/Accenture-Pulse-Check-Dive-Key-Findings-Personalized-Experiences.pdf

Shapiro, A., Levitt, M., & Intagliata, C. (2022, September 9). *How the polarizing effect of social media is speeding up*. NPR. Retrieved September 19, 2022, from https://www.npr.org/2022/09/09/1121295499/facebook-twitter-youtube-instagram-tiktok-social-media

Shin, T. (2020, June 2). *A Beginner-Friendly Explanation of How Neural Networks Work*. Towards Data Science. Retrieved September 14, 2022, from https://towardsdatascience.com/a-beginner-friendly-explanation-of-how-neural-networks-work-55064db60df4

Spillane, J. (2018, August 15). *How GDPR Can Undermine Personalization and User Experience*. Business 2 Community. Retrieved September 14, 2022, from https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

Ved, A. (2019, February 28). *How to develop Artificial Intelligence that is GDPR-friendly*. TechGDPR. Retrieved September 14, 2022, from https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/