**DataPulse Innovations and Personalization Technologies Corporation**

**Thomas Martin**

**CS-370-11456-M01 Current/Emerging Trends in CS**

**Southern New Hampshire University**

**4-2 Project One Submission**

**July 25, 2024**

Abstract

At DataPulse Inc., our mission is to revolutionize the online experience by leveraging advanced neural network technologies to create deeply personalized and engaging user interactions. We are committed to enhancing user satisfaction by delivering tailored content, fostering meaningful connections, and providing relevant recommendations. Our dedication to transparency, privacy, and ethical data practices ensures that we not only meet but exceed the expectations of our users and regulatory standards. By putting users first, we aim to build a trusted digital environment that empowers individuals and drives innovation in social networking. DataPulse Inc. has set the standard for personalized online interactions. Our mission is to create deeply personalized and engaging user experiences that keep our users connected and entertained.

**Contents:**

1. Introduction ………………………………………………………………………3

2. Storage limitation

2.1 Principle of Storage Limitation……………………………….……….3-4

2.1.1 Data Retention Policies……………….……………………….4

2.2.2 Secure Deletion Practices………………….………………......4

3. General Data Protection Regulation

3.1 Transparency…………………………………………………………….5

3.1.1 Explanation……………………………………………………5

3.1.2 Implication…………………………………………………….5

3.2 Purpose Limitation

3.2.1 Explanation…………………………………………….……5-6

3.2.2 Implication…………………………………………………….6

3.3 Data Minimization

3.3.1 Explanation…………………………………………………….6

3.3.2 Implication……………………………………………….…….6

3.4 Accuracy

3.4.1 Explanation…………………………………………………….6

3.4.2 Implication…………………………………………….……….7

4. Confidentiality…………………………………………………….……………….7

5. Accountability……………………..………………………………………………8

**1. Introduction**

**About DataPulse Inc.**

DataPulse Inc. is a pioneering social networking company at the forefront of user experience innovation. Leveraging advanced neural network algorithms.

Neural networks are a type of artificial intelligence inspired by the human brain. They are designed to recognize patterns and classify objects based on the data they receive. Neural networks consist of multiple layers. These layers provide the building blocks of the network. The input layer is the first layer in a neural network. It receives raw data, such as images, text, or other inputs. The input layer deciphers the way the information is processed. Each unit in this layer represents a different feature of the data. The hidden layers are the intermediate layers between the input and output layers. These layers do the heavy lifting of processing the input data. They consist of multiple neurons that are connected to the neurons in the previous layer. The output layer is the final layer of the neural network. It provides the result of the network’s processing.

**2. Storage Limitation**

**2.1 Principle of Storage Limitation**

Under the GDPR, personal data must only be retained for as long as it is necessary to fulfill the purposes for which it was collected. This principle prevents organizations from storing data indefinitely and mandates that data no longer needed must be securely deleted.

**2.1.1 Data Retention Policies**

DataPulse Inc. is a leading social networking company that excels in delivering personalized user experiences. By utilizing advanced neural network algorithms, DataPulse can anticipate and cater to the needs of its users. Our platform offers tailored recommendations, including suggested posts, friend requests, groups to join based on shared interests, relevant news articles, engaging discussions, and interactive games. This high level of personalization is integral to our business model, ensuring that users find content that resonates with them, thereby enhancing their overall experience and engagement on the site.

DataPulse Inc. must establish clear retention periods for different types of personal data based on the specific purposes for which they were collected. Data used for short-term personalization might have a shorter retention period than data used for long-term user preferences. DataPulse Inc. must implement regular review processes to identify and delete data that is no longer necessary for personalization purposes. Automated systems may be used that monitor data age and trigger deletion protocols. DataPulse Inc. must ensure that data retention periods align with the purposes disclosed to users.

**2.2.2 Secure Deletion Practices**

DataPulse Inc. must develop and implement procedures for securely deleting personal data. This can include methods like data wiping, degaussing, and physical destruction of storage media. DataPulse Inc. must verify that data has been completely and securely deleted. Maintain documentation of deletion processes and verification steps as part of compliance records.

**3. General Data Protection Regulation**

**3.1 Transparency**

**3.1.1 Transparency Explanation**

Transparency in GDPR refers to the principle of being clear, open, and honest with people from the start about who you are, and how and why you use their personal data. Transparency is important even when you have no direct relationship with the individual and collect their personal data from another source.

Transparency is more than just being clear, open, and honest with people, individuals who have the right to be informed about the collection and use of their personal data. You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.

**3.1.2 Transparency Implication**

DataPulse must provide clear, concise, and easily accessible privacy notices on the website and app. Develop interfaces that allow users to easily give consent, manage their data, and understand how their information is being used. Maintain and regularly update privacy notices to reflect any changes in data processing practices.

**3.2 Purpose Limitation**

**3.2.1 Purpose Limitation Explanation**

Data should only be collected for specific, explicit, and legitimate purposes and not used in ways that are incompatible with those purposes. Data collected must be for the pre-specified purpose and not archived for future, unspecified uses. DataPulse practices should ensure that data is only used for the intended and disclosed purposes.

**3.2.1 Purpose Limitation Implication**

DataPulse must clearly define and communicate the specific purposes for which user data is collected, such as improving personalization of user experiences and targeted advertising. Data collected for one purpose cannot be repurposed for another without obtaining further user consent. The company must document the purposes for data collection and ensure that any data processing aligns with those purposes. Regular audits should be conducted to ensure compliance.

**3.3 Data Minimization**

**3.3.1 Data Minimization Explanation**

Only the data necessary for the specified purposes should be collected. We need to review our data collection processes to ensure we are not gathering more information than required.

**3.3.2 Data Minimization Implication**

DataPulse must evaluate and limit the data it collects to only what is needed for personalization. Excessive data collection should be avoided to comply with this principle.

**3.4 Accuracy**

**3.4.1 Accuracy Explanation**

Under the GDPR, personal data must be accurate and, where necessary, kept up-to-date. This means that organizations have a responsibility to ensure that any personal data they process is correct and to rectify any inaccuracies promptly.

**3.4.1 Accuracy Implication**

DataPulse must Implement regular checks and updates to ensure the accuracy of the data used for personalization. This includes cross-referencing user input with other reliable sources and using algorithms that can detect and correct discrepancies. GDPR allows the utilization of automated systems that can regularly validate data accuracy, flagging inconsistencies and prompting updates where necessary.

**4. Confidentiality**

Under the GDPR, organizations must ensure that personal data is processed securely, protecting it from unauthorized access, breaches, and other security threats. This principle is crucial for maintaining the trust of users and complying with legal requirements. Staying compliant requires up to date and advanced best practices such as Federated Learning. This approach allows models to be trained across multiple devices or servers holding local data samples, without exchanging them. It keeps the data localized and only shares model updates, enhancing privacy. DataPulse current robust security protocols provide a strong foundation for protecting user data. Enhancing these measures further ensures compliance and builds user trust.

**5. Accountability**

Accountability is one of the key principles in data protection law – it makes you responsible for complying with the legislation and says that you must be able to demonstrate your compliance. DPR mandates that organizations demonstrate compliance with data protection principles and take responsibility for their data processing activities. Accountability includes appointing a DPO to oversee compliance efforts and manage data protection activities. Regularly train employees on GDPR requirements and data protection best practices. Conduct regular audits to ensure adherence to GDPR principles and address any compliance gaps promptly.

**References:**

Information Commissioner's Office. (n.d.). Right to be informed. Retrieved July 27, 2024, from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-be-informed

GDPR-Info.eu. (n.d.). Recital 58 – Information to be provided on personal data. Retrieved July 27, 2024, from https://gdpr-info.eu/recitals/no-58/

GDPR.eu. (n.d.). 7 main data protection principles under GDPR. Retrieved July 27, 2024, from https://www.gdpreu.org/7-main-data-protection-principles-under-gdpr/