

**Memorandum to Governor Karras, State of Mongo**

Janae Craig

Old Dominion University

CYSE 406

Professor Cheney

March 24, 2023

**MEMORANDUM**

DATE: March 24, 2023

TO: Governor Karras, State of Mongo

FROM: Janae Craig

SUBJECT: The Need for Cyber Law in the State of Mongo

**Concerns, Importance, and Individual care**

Concerns about the usage, distribution, and preservation of private information in different manifestations, such as text, photos, sounds, and video, are referred to as data protection and confidentiality of information. With the development of technology and the exponential increase in data collection and processing, these problems have assumed growing importance (Goldsmith, 2013).

Because they guarantee that people have control over and discretion over the use of their personal information, information security and privacy are crucial. Misuse or improper handling of this information can have various detrimental effects, including identity fraud, fraudulent transactions, and reputation damage. Additionally, laws governing data protection and confidentiality assist in stopping companies and organizations from utilizing information about individuals in illicit or unethical ways (Caproni, 2011).

Individuals must consider data protection and security mechanisms to protect themselves from potential harm. Likewise, businesses and organizations must prioritize security protocols and privacy to maintain customer trust and compliance.

**Helpful Definitions and Examples**

**Biometric data:** any information about a person's physical, biological, or behavioral characteristics that can be used to identify that person. Voice recognition, iris scanning, facial recognition, and fingerprint scanning are a few examples.

**GDPR:** A set of laws governing data privacy and protection known as GDPR, or the General Data Protection Regulation, went into force in the European Union in 2018. For example, by establishing stringent guidelines on how businesses must gather, use, and keep personal data, it strives to safeguard the confidential data of EU individuals.

**PII:** Any information used to identify a specific person is known as Personally Identifiable Information, or PII. A few examples are whole names, birthdates, SS numbers, passport details, license plate numbers, and biometric information like fingerprints or image recognition.

**Anonymization:** The process of deleting or encrypting characters from data to make it unattainable to determine a person is known as the anonymization of personal data, for instance, substituting a person's name with a special ID number or combining information from others to avoid identification.

## **Laws for the State of Mongo**

Laws safeguarding particular categories of personal data, such as biometric data, internet search history, and geolocation data, may be passed by a state legislature. For information about health, economics, and education not already protected by federal law, they might offer further protections.

### **GDPR feasibility**

I would request a deep introspection on the feasibility of GDPR, but it has a few pros and cons associated with it.

#### **Positives**

- Better personal data security for EU citizens
- Increased responsibility and openness for businesses that gather and use personal information.
- More personal control over their personal information, such as the capacity to inspect, amend, and delete it.
- Higher penalties for businesses that disregard GDPR laws, which may serve as a deterrent to non-compliance.
- Collaboration in safeguarding information laws among citizens will make operations for multinational corporations in the area simpler.

#### **Negatives**

- Organizations' costs of adherence, particularly for smaller firms.
- GDPR standards and how they relate to particular industries and circumstances are unclear.
- Innovation and research could be hindered by GDPR limits, which could prevent the use of private information for specific reasons.
- Challenges in implementing GDPR requirements, especially against firms outside the EU.
- Possibility of adverse effects for non-EU nations, who would see their accessibility to EU merchandise restricted as a result of GDPR compliance rules.

Given all of the facts, laws such as GDPR should be enacted in the state. These are critical issues for the citizens of Mongo as well as the government.

Thank You,

Janae Craig

Aide to Governor, State of Mongo

## References

- Caproni, V. (2011). Surveillance and transparency. *American Criminal Law Review*, 48(3), 1017-1054.
- Goldsmith, J. (2013). The cyberthreat, government network operations, and the Fourth Amendment. *Harvard National Security Journal*, 4(1), 1-68.