Privacy Memorandum

Sarah Vakos

CYSE 406 36889

07/19/2022

MEMORANDUM

Date: July 19, 2022

To: Governor Karras, State of Mongo

From: Sarah Vakos

Subject: Proposed Privacy Laws

Data protection and privacy issues include sensitive information of consumers, employees and shareholders that businesses handle. Sensitive information includes full name, dates of birth, addresses, credit card information, etc. Businesses can do whatever they want with the sensitive data if there are no laws in place. If there is no safeguard in place of PII then data can get lost, stolen or distributed to other businesses. Businesses can sell the information to third parties and what they do with that information is their choice, they can use the sensitive data to commit crimes like identity fraud. Constituents should care because it could happen to them, by using a consumer's name and bank account information, they can act like them and buy whatever they desire or apply for credit cards which places the consumer at risk by putting them in debt for something they did not intentionally buy. After all the damage is done their reputation is ruined and they must start from the beginning again to get their reputation back to its original state. Why should you care? Because this very example can happen to you or your family. Another issue is the consumers, employees and shareholders losing their trust in the business that they had their information stored with. It puts a foul taste in their mouth which can be a bad look for the business.

Some important terms to know when proposing laws for privacy and data protections include biometric data. This is any data about a person's human genome, facial structure, fingerprints, and even behavioral characteristics. Biometric data is used to identify a specific person. PII is also known as personally identifiable or identifying information, which is the sensitive data I described above, full name, dates of birth, addresses, credit card information along with social security numbers, driver license number, email addresses, etc. Your PII is stored in accounts you have like insurance and medical billing to social media accounts. GDPR is General Data Protection Regulation, this is what the EU uses as their privacy laws. It protects personal data which is defined on page 243 in the Cyber Law 406 textbook, Cybersecurity and Privacy Law in a Nutshell by Jay P. Kesan and Carol M. Hayes as, "location data, online identifiers, and "factors subject to the physical, physiological, genetic, mental, economic, cultural or social identity" of the data subject". GDPR applies to people in the EU just visiting on vacation and it applies to any organization doing work with businesses in the EU as well. Under GDPR, consumers in the EU have more rights than consumers in the US because they can opt-out of data sharing with third parties, request that their data be deleted forever, and they are immediately notified when they are involved in a breach.

Specific types of personal data that should be included in the State of Mongo legislature in addition to data not already protected by federal law are race, political standpoint, religious beliefs, and health data. Race would be what you fall under including but not limited to, White, Black, African American, American Indian etc. A person's political standpoint can be democrat, republican or less popular parties like libertarians and constitution party. Religious beliefs can be Christian, Islam, Buddhism or even Atheist, believing in no god. Health data would include your blood type, diagnosis, medications, lab results and shot records. All these specific types of data are all important in identifying a person. It is the type of data you don't want anyone else knowing or be able to easily access or get ahold of without proper authorization or consent. Consent is defined as getting the okay from the individual for something to happen like obtaining sensitive information.

The pros outweigh the cons for applying GDPR practices. Pros include a better relationship or bond with consumers and businesses, since they have full control of how their data is handled and they have increased data privacy and security. If data isn't processed correctly or a breach occurs, businesses and organizations get fined for not following procedure and taking care of consumers data accurately. Cons include large businesses having to hire data protection officers and companies who want to do business with companies in the EU have to follow GDPR regulations. This can turn businesses away from the EU. Applying GDPR practices to your legislature for the State of Mongo would benefit your citizens and constituents by upholding the best privacy procedures for data protection. This would also decrease the number of complaints you receive from constituents about their data not being secured and being sent to other organizations without their consent because they would have full control of their information and have the option to opt-out of data sharing.

Reference Page

1. Kesan, Jay P., and Carol M. Hayes. “Chapter 12 Privacy Law and Data Protection.” *Cybersecurity and Privacy Law in a Nutshell*, West Academic Publishing, St. Paul, MN, 2019, p. 243.