**Weekly Assignment 6**

If you don’t know what CCPA is, read this:

<https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act>

A copy of the real CCPA regulations is included here:

<https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>

Use the CCPA regulations pdf above as a guide to answer the following questions:

1. Does a US company need to worry about these regulations? If so, why? If not, why not?

Yes, a US company needs to worry about GDPR regulations if it engages in activities that fall under the scope of the GDPR. Specifically, a US company must comply with GDPR if it:

* **Offers goods or services to individuals in the EU**: This includes businesses that actively market their products or services to EU residents, regardless of whether the services are free or paid.
* **Monitors the behavior of individuals in the EU**: This includes tracking EU residents’ behavior on the internet, such as using cookies to track online activity for behavioral advertising purposes.

Failure to comply with GDPR can result in substantial fines and damage to the company’s reputation, making it crucial for US companies with any EU interactions to be aware of and adhere to these regulations.

1. Which section number lists the penalties for non-compliance? How much are those amounts?

 For less severe infringements, the fine can be up to 2% of the company’s total worldwide annual turnover of the preceding financial year, whichever is higher.

 For more severe infringements, the fine can be up to 4% of the company’s total worldwide annual turnover of the preceding financial year, whichever is higher.

1. What do the regulations say about a unique identifier?

GDPR defines a unique identifier as personal data when it can be used to directly or indirectly identify an individual. This includes identifiers such as names, identification numbers, location data, online identifiers (e.g., IP addresses), or any other data that can be linked to an individual.

Under GDPR, processing of unique identifiers must comply with data protection principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

1. How do these regulations affect a business (that earns more than $25 million a year) who requires customers to use their email to login to their website? Based on these regulations what changes, if any, might the business need to make to their website to satisfy the regulations?

For a business that earns more than $25 million a year and requires customers to use their email to log in to their website, the following changes and considerations are necessary to comply with GDPR:

* **Data Protection by Design and Default**: Ensure that data protection is considered and integrated into the development of business processes and website functionalities from the start.
* **Legal Basis for Processing**: Establish and document the legal basis for processing customers’ email addresses (e.g., consent, contract necessity).
* **Consent**: If processing is based on consent, ensure that it is obtained in a clear, informed, and unambiguous manner. Customers must be able to easily withdraw consent.
* **Data Minimization and Purpose Limitation**: Collect only the necessary data for the specific purpose (e.g., login functionality) and ensure it is not used for any other purpose without further consent.
* **Transparency and Information**: Provide clear and comprehensive information to customers about how their email addresses and any other personal data will be used. This includes updating privacy policies and providing notices at the point of data collection.
* **Rights of Data Subjects**: Implement mechanisms to allow customers to exercise their rights, such as accessing their data, requesting corrections, and requesting data deletion.
* **Data Security**: Implement appropriate technical and organizational measures to ensure the security of personal data, such as encryption and secure storage.
* **Data Breach Notification**: Establish procedures to detect, report, and investigate personal data breaches. Notify the relevant supervisory authority within 72 hours of becoming aware of a breach, and inform affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

To comply with these requirements, the business may need to:

* Update their privacy policy and terms of service.
* Implement or enhance consent mechanisms for data collection.
* Ensure secure data handling practices.
* Provide easy access for users to manage their data and preferences.
* Conduct regular audits and assessments to ensure ongoing compliance.

These steps will help ensure that the business aligns with GDPR requirements and mitigates the risk of non-compliance penalties.

When you are finished upload this document into Canvas for your submission.