In-Class Exercise 8
Kompliance Krew
State of Wisconsin - Data Breach Policy

1. Summary:

The Wisconsin statute (134.98) requires entities (businesses, government bodies, and organizations) operating in Wisconsin to notify individuals if unauthorized persons have acquired their personal information. The law outlines which types of information are considered personal, the actions that must be taken during a data breach, and specific timeline notifications. It also details exemptions and ensures no local regulations conflict with the state's rules.

2. Definitions:

Entity: Any organization, except an individual, that:

- Conducts business in Wisconsin.
- Licenses personal information in Wisconsin.
- Maintains personal or financial information for Wisconsin residents.
- Includes government bodies, businesses, financial institutions, and organizations.

Name: An individual's last name combined with their first name or first initial.

Personal Information: Includes a person's first name (or initial) and last name combined with one or more of the following:

- Social Security number.
- Driver's license or state ID number.
- Financial account numbers (e.g., debit/credit card) or any related security credentials (e.g., access codes).
- DNA profiles.
- Biometric data (e.g., fingerprints, voice print, retina scan).

Publicly Available Information: Information lawfully made available through media or public records in Wisconsin.

3. What info/data needs to be protected?

The following personal information is protected under this statute for the state of Wisconsin:

- Full name or initial with the last name combined with:
  - Social Security number
  - Driver's license or state ID number
  - Financial account numbers or security access codes
  - DNA profiles
  - Biometric data (e.g., fingerprints, retinal scans)

This information must be protected if it is not publicly available and is unencrypted or unaltered.

4. Definition of Breach

A breach occurs when personal information is acquired by an unauthorized person,

meaning someone who does not have permission from the entity that holds the data. The acquisition is considered a breach if it poses a risk of identity theft or fraud.

5. Actions to be taken

- Entities must notify affected individuals as soon as they become aware of the breach, within a reasonable time frame, but no later than 45 days after discovering it.
- Notifications must be provided by mail or through previously established communication channels.
- If over 1,000 people are affected, consumer reporting agencies must also be notified.
- No notification is required if there is no material risk of identity theft or if the breach occurred in good faith (e.g., by an employee using it lawfully).

6. Other Regulations

- **Regulated Entities Exempt**: Entities that comply with federal privacy and security laws (e.g., financial institutions under 15 USC 6801-6827 or health entities under 45 CFR 164) are exempt from this law.
- **Law Enforcement Requests**: Law enforcement can request that notification be delayed if it would interfere with an investigation or homeland security.
- **Preemption of Local Regulations**: Cities, villages, and counties cannot enact separate laws regarding the disclosure of unauthorized personal information.
- **Federal Preemption**: If federal legislation is enacted with similar requirements, the state law may become inapplicable.