Cognitive Automation Labs

# Cognitive Automation Labs Data Interpretation and Classification Guide

As part of our commitment to safeguarding the privacy and security of our data, it is essential for us to always be cognizant of the type of data that we are working with and understand the level of sensitivity by its nature. By categorizing data into sensitive and non-sensitive categories, we can ensure appropriate levels of protection and compliance with relevant privacy regulations. This memo serves as a guideline for data classification and provides an overview of how to differentiate between sensitive and non-sensitive data.

## Sensitive Data:

- Sensitive data refers to information that, if disclosed or compromised, could result in harm, legal ramifications, or significant damage to individuals or the organization. It typically includes, but is not limited to, the following types of data:
- Personally Identifiable Information (PII): Any data that can be used to identify an individual, such as full name, social security number, driver's license number, passport number, or financial account information.
- Protected Health Information (PHI): Any data related to an individual's medical history, treatment, or health condition that is protected by HIPAA (Health Insurance Portability and Accountability Act) regulations.
- Financial Data: Any data related to financial transactions, bank account details, credit card information, or other sensitive financial information.
- Intellectual Property: Any proprietary or confidential information, including trade secrets, patents, copyrights, or any other information that provides a competitive advantage to the organization.
- Legal or Compliance-related Data: Any data subject to legal or regulatory requirements, including legal documents, court orders, or any information that must be protected due to legal obligations.
- Client-Related Data: Any data specifically associated with our clients, including client names, contact information, transaction history, or any other data provided by clients in the course of our business relationship.

## Non-Sensitive Data:

- Non-sensitive data refers to information that, if disclosed or compromised, would not cause significant harm or legal consequences to individuals or the organization. It includes general business information that is publicly available or does not contain personal, financial, or confidential details. Some examples of non-sensitive data are:
- Publicly Available Information: Information that is accessible to the public, such as general marketing materials, press releases, or public domain data.
- General Business Information: Data related to routine business operations, such as internal memos, meeting minutes, or non-confidential reports.
- Non-Identifiable Data: Data that has been anonymized or stripped of any personally identifiable information, rendering it non-sensitive.

## Data Classification Guidelines:

To ensure consistent and accurate classification of data, please follow these guidelines:

- Understand the Context: Consider the nature and purpose of the data to determine its sensitivity. Evaluate if the data falls within the categories of sensitive or non-sensitive as outlined above.
- Apply the Principle of Least Privilege: Limit access to sensitive data only to individuals who require it for their job responsibilities. Non-sensitive data may have broader access within the organization.
- Use Encryption and Secure Storage: Sensitive data should be encrypted and stored securely to prevent unauthorized access or breaches.
- Follow Data Handling Procedures: Adhere to data handling procedures, including proper disposal of sensitive data, use of secure communication channels, and adherence to relevant data protection policies.
- Report Suspected Data Breaches: If you suspect a data breach or unauthorized access to sensitive data, report it immediately to the designated IT security or data protection team.
- Remember, data classification is crucial for maintaining the privacy, security, and compliance of our organization. Client-related data is classified as sensitive data due to its potential impact on our clients and the importance of maintaining their trust.

| | |
|---|---|
| Prepared by: | Joanne Parsons – Head of Business Administration |
| Approved by: | Jonathan Parsons – Co-Founder & CEO |
| Last Modified: | 11/10/2022 |