Personally Identifiable Information (PII) Safeguarding Policy

Contents

Purpose 1
Scope 1
Identifying PII 1
1. Public PII 2
2. Protected PII 2
Maintaining PII 3
Enforcement 4
Exceptions 4

MENU's employees, in the course of their normal job responsibilities, will come into contact with Personally Identifiable Information (PII). It is important for employees to understand their roles in the collection and storage of PII.

Purpose

The purpose of this procedure is to provide details on how to identify and handle Personally Identifiable Information (PII), the process of securely storing any PII that the organization is required to maintain, and what to do in the event of a disclosure of PII.

Scope

All staff, employees and entities working on behalf of MENU who are using MENU-owned or personally-owned computer or workstations that are connected to the MENU network are subject to this procedure.

Identifying PII

Personally Identifiable Information (PII) is information, which can be used to distinguish or trace an individual's identity, such as his/her name, social security or passport number, biometric records or other personal information alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name or other personal information.

There are two (2) types of Personally Identifiable Information (PII) and identification of each type will dictate the actions needed to ensure its safety and integrity.

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

1. Public PII

This is information that is available in public sources such as public websites, employee directories, telephone books or other similar public sources. The following information can be considered Public PII:

- First and Last Name
- Address
- Work Telephone Number
- Work email address
- Home telephone number
- General educational credentials
- Photos and videos

2. Protected PII

This is defined as any information which, if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. It includes any one or more of the types of information that are outlined below:

- Passport number
- Social Security Number
- Username and password
- Passport number
- Alien registration number
- Credit card number
- Clearances
- Banking information
- Biometrics
- Date and place of birth
- Mother's maiden name
- Criminal, medical and financial records
- Photos and video including any of the above

MENU currently collects the following information:

- First and last name
- Email address
- Language
- Phone number
- Payment methods (stored with PCI-compliant third-party)
- Orders
- Device ID
- Redemptions
- Loyalty points

- Social ID
- Location coordinates
- Address (for delivery orders)
- Favorites
- Dietary information.

Maintaining PII

During the course of normal job responsibilities, employees may come in contact with either Public or Protected PII, either already existing in the MENU network, or as part of a business process. Because Protected PII requires special handling due to potential risk associated with its disclosure, it is important to

1) verify the need for the existence of PII in the MENU network and
2) ensure that the information is properly secured.

- ***Verifying the need to collect PII***

Based on best practice MENU only collects the least amount of information in order to follow standard business procedures. MENU applies caution when collecting Protected PII and periodically reviews the collected information, and if deemed unnecessary, alters the procedures.

- ***Collection Procedures***

If PII does need to be collected, employees have certain responsibilities in making sure the data is secured. Any written information as a result of a phone conversation must be destroyed via shredding. Physical files that contain PII need to be locked in a secure cabinet or room when not being actively viewed or modified. Any PII data collected must not be stored on the local workstation; it would need to reside in GoogleDrive, where it is encrypted and backed up.

- ***Verifying the need to store PII***

Whenever PII is found residing in the MENU network, a determination needs to be made regarding whether the information is needed for an existing business practice, or if it can be securely disposed. If the information does need to be retained, please contact MENU Directors for guidance on the best means to secure or dispose of the information properly.

- ***Authorized dissemination of PII***

In the event an outside entity would need to have any data that includes Protected PII, said entity would need to confirm that they understand the sensitivity of the information, and the need to properly safeguard it. Once it leaves the MENU network, the Data Security Management cannot guarantee its security. Transport of data should be done through secure means (ideally shared through GoogleDrive; otherwise encryption or secured transport are necessary).

- ***Unauthorized dissemination of PII***

In the event of an unauthorized disclosure or access of PII:

- Report the incident to your direct supervisor
- Send an email to [privacy@menu.app]
- Do NOT forward any compromised information in the email
- Include the location of the information (email or network location)
- If email, include the sender and subject (unless the subject contains the PII)
- Include any other relevant details, such as location and contact phone number
- Comply with the instructions from the Incident Response Team

Enforcement

This policy is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination of employment.

Exceptions

Limited exceptions to the procedure must be approved by MENU Security Management.