„Privacy by Design“ Guidelines

Contents

Context

The privacy of our customers’s data is our primary priority. Customer’s entrust us with a lot of data and it is our responsibility to make sure we treat it safely, always keeping their privacy in mind, in order to preserve that trust.

Our goal is to make it as convenient & easy for a customer to order from anywhere, at any time, and to personalize their experience to make sure they return and become loyal to the brand. While working towards this goal we want to keep our customers informed about how we use their data to provide them with a better experience. Keeping customers in the loop is integral to building a loyal customer base, and making sure they don’t feel betrayed or misinformed.

This document aims to establish guidelines that should be followed by each team member when building new products & new functionality, in order to make sure our customer’s privacy is respected in all of our endeavours.

The 7 Principles of “Privacy By Design”

1. Proactive not Reactive; Preventative not Remedial

- We consider privacy & security aspects at the start of new product initiatives, not as an add-on at the end.
- We make sure already during the development that the intitiative will keep customer’s data private & secure

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

- We speak out if we have concerns to how customer data is being / will be treated
- We ask ourselves how the feature will work if less or no customer data is available. *How will this feature behave if the customer chooses to delete his account? How will this feature work if he objects to the personalization of his experience?*

2. Privacy as the Default

- Personal data should be automatically protected in new features
- By default, new features should use the least amount of data possible
    - We only collect data that we need to process to achieve the objective of a feature
- The customer has to opt-in to expose more data
- A customer has to opt-in to the processing of personal data to personalize his experience

3. Privacy Embedded into Design

- Privacy should be *"integral to the system, without diminishing functionality" (Ann Cavoukian, Ph.D)*
- Making user experiences worse for the sake of privacy is not an option. Privacy needs to be integrated in a holistic way.

4. Full Functionality – Positive Sum, not Zero Sum

- Trade-offs shouldn't have to be made to accommodate privacy
- By treating privacy as important as business objectives when building new features it is possible to build great products that account for both

5. End-to-end security – Full Lifecycle Protection

- Personal data has to be treated securely & privately from the moment it is collected to the moment it is destroyed
- Personal data has to be encrypted in transit through use of TLS
- Personal data has to be encrypted at rest using state-of-the-art encryption technologies
- Personal data can only be accessed by authorized team members and only for reasons accounted for during development

6. Visibility and transparency – Keep it open

- We aim to be transparent during personal data collection, letting the customer know why we need the data

7. Respect for User Privacy – Keep it user-centric

- Privacy is our primary priority and it is always at the center of attention