Privacy Impact Assessment Template

24 Feb 2023 / Chloe Wright

Complete

Score	0%	Flagged items	0	Actions	0

Created on	24.02.2023 14:30 PST
Project Manager/System Owner	Chloe Wright
Location	California, USA (36.778261, -119.4179324)

Project/System Information

Project/System Title

PIA for New Processes

Description

This document details our PIA program to help our organization deal with potential risks and implications of data privacy and security for our business processes, particularly during or if we need to introduce new ones.

Purpose

To set out the process for completing Privacy Impact Assessments (PIAs) with the aim of identifying any impact on privacy whenever a new service, system, or process is introduced

What specific legal authorities, arrangements, and/or agreements require the collection of this information?

- Department of Information Privacy
- Privacy Act

Data in the System

What data is to be collected?

- Customer demographics
- Customer profiles

What are the sources of the data?

- Lead generation tools
- Opt-in marketing communications
- Focus Group Discussions (FGDs)

Why is the data being collected?

To improve the way we produce, market, and sell our company's products and services

What technologies will be used to collect the data?

- Lead generation tools
- Website tracking technologies (cookies)
- Social media listening tools

Does a personal identifier retrieve the data?	Yes

Attributes of the Data (use and accuracy)

Describe the uses of the data.

- Optimized marketing communications and collaterals

- Strategic business decisions on financial aspects
- Personalized advertisements and campaigns

Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?	Yes

How will the data collected from individuals or derived by the system be checked for accuracy?

- Using our company's unique data filtering program
- Letting the data collected go through a rigorous process of initial screening using technologies to be leveraged by our dedicated data processing team

Sharing Practices

Will the data be shared with any internal or external organizations?	Yes

How is the data transmitted or disclosed to the internal or external organization?

- Internal: Limited access to the senior leadership level as well as managers (with exemptions for customer-facing teams)
- External: Limited access to identified stakeholders

How is the shared data secured by external recipients?

Only through a secure dashboard with 2-layer authentication (cloud storage)

See attached PDF file for the updated guidelines on sharing data with external recipients.

Updated Guidelines on External Data Sharing [2023].pdf

Notice to Individuals to Decline/Consent Use

Was notice provided to the different individuals prior to collection of data?	Yes
Do individuals have the opportunity and/or right to decline to provide data?	Yes
Do individuals have the right to consent to particular uses of the data?	Yes

Access to Data (administrative and technological controls)

Has the retention schedule been established by the Records Officer? If so, what is the retention period for the data in the system?	Yes

The retention period for the data in the system is 5 years.

What are the procedures for identification and disposition of the data at the end of the retention period?

Since these are complex and regularly updated, refer to the attached reference document for such procedures.

Procedures for Data Identification and Disposition.pdf

Describe the privacy training provided to users, either generally or specifically relevant to the program or system?

The attached files outline both the general and specific privacy training programs provided. Currently, the data security and privacy team is responsible for these efforts.

General Privacy Training.pdf

Specific Privacy Training.pdf

Is the data secured in accordance with Federal Information Security Management Act (FISMA) requirements?	Yes

Provide date that the Certification & Accreditation was completed

January 20, 2019
Control number 01202019-CN

Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

1. General organization access to all customer data can lead to internal privacy breaches. This is then mitigated by introducing a system wherein only relevant teams and personnel have full access to these data as crucial to the nature of their work.
2. Use of tools, software, and technologies that have zero to limited layers of security can lead to inefficient data security measures. Recently (December 2022), our IT and network security team spearheaded the initiative of upgrading the authentication and controls that our tools have to help us ensure the safe processing and storage of the data we collect.

Completion

Other comments and notes

- Reference documents have been attached to this report for further context.
- Regular updates on the procedures for data identification and disposition are a must. Coordinate with the Chief Information Officer for the next scheduled annual review in March 2023.

Project Manager/System Owner

Chloe Wright
24.02.2023 15:01 PST

Chief Privacy Officer

Lance Alvarez
24.02.2023 15:02 PST

Chief Security Officer

Stuart Brand
24.02.2023 15:03 PST

Chief Information Officer

Kris Croft
24.02.2023 15:04 PST

Appendix

Updated Guidelines on External Data Sharing [2023].pdf

Procedures for Data Identification and Disposition.pdf

General Privacy Training.pdf

Specific Privacy Training.pdf