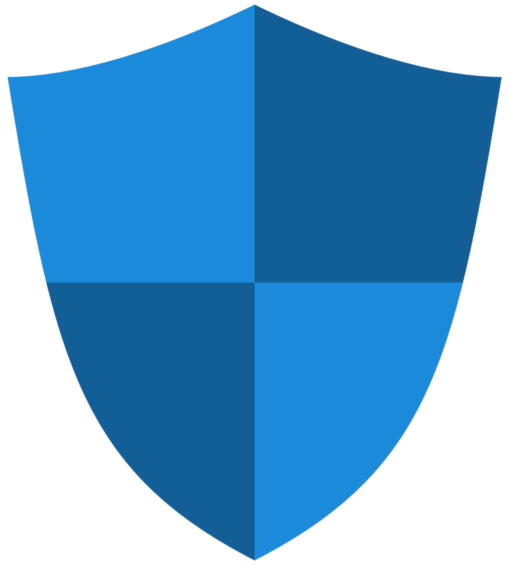
SHOPSMART COMPANY

SHOPSMART: PRIVACY-CENTRIC CUSTOMER REWARDS PROGRAM

Applying Privacy-by-Design and GDPR to a customer rewards system



PRESENTED BY :

DIVYAVAAHINI THYAGARAJAN

Introduction of Company and Dataset

ShopSmart is a **retail platform** launching a **customer rewards program** that offers personalised discounts and reward points. The goal is to increase **customer loyalty**
while keeping privacy as the main design principle.

Key Points:

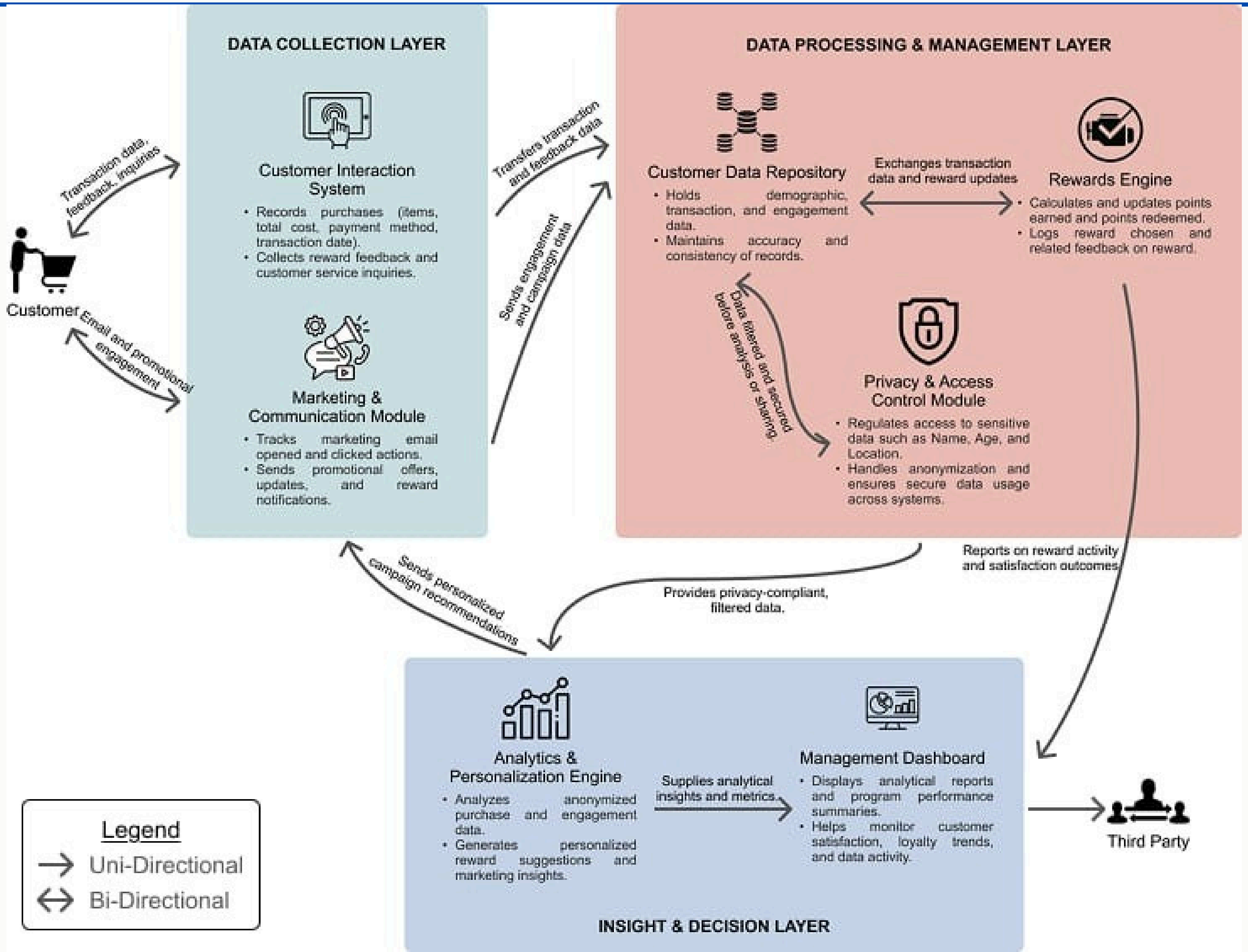
- Customer **privacy** and **safe data management** first
- Offers **personalised rewards** without exposing sensitive information
- Reduces **customer's worries** about sharing data with the program
- Avoids risks such as **unauthorised access** and **data leaks**

Data Overview (customer_rewards_data.csv)

- 500 records, 16 attributes
- **Direct identifier:** Name
- **Quasi-identifiers:** Age, Location, Gender
- **Indirect / transactional data:**Transaction Date, Items Purchased, Quantity, Total Cost,Payment Method, Points Earned, Points Redeemed, Reward Chosen,Feedback on Reward, Marketing Email Opened/Clicked, Customer Service Inquiry

SHOPSMART COMPANY

Explanation of System Model Diagram



DATA COLLECTION LAYER

Customer Interaction System

- Records purchases (items, total cost, payment method, transaction date).
- Collects reward feedback and customer service inquiries.

Marketing & Communication Module

- Tracks marketing email opened and clicked actions.
- Sends promotional offers, updates, and reward notifications.

DATA PROCESSING & MANAGEMENT LAYER

Customer Data Repository

- Holds demographic, transaction, and engagement data.
- Maintains accuracy and consistency of records.

Rewards Engine

- Calculates and updates points earned and points redeemed.
- Logs reward chosen and related feedback on reward.

Privacy & Access Control Module

- Regulates access to sensitive data such as Name, Age, and Location.
- Handles anonymization and ensures secure data usage across systems.

INSIGHT & DECISION LAYER

Analytics & Personalization Engine

- Analyzes anonymized purchase and engagement data.
- Generates personalized reward suggestions and marketing insights.

Management Dashboard

- Displays analytical reports and program performance summaries.
- Helps monitor customer satisfaction, loyalty trends, and data activity.

Legend

→ Uni-Directional

↔ Bi-Directional

Customer
Transaction data, feedback, inquiries
Email and promotional engagement
Transfers transaction and feedback data
Sends engagement and campaign data
Exchanges transaction data and reward updates
Data filtered and secured before analysis or sharing
Reports on reward activity and satisfaction outcomes
Provides privacy-compliant, filtered data.
Sends personalized campaign recommendations
Supplies analytical insights and metrics.
Third Party

Perform Data Privacy by Design Strategies

- **Database Minimizing - Identifiability, Linkability (Legitimate Interest)**

Limit data collection (e.g., use IDs instead of names) to reduce identifiability and linkability of customers while still supporting reward operations.

- **Reason Specification - Unawareness, Non-compliance (Legal Obligation)**

Clearly stating why each data point is collected reduces user unawareness and supports compliance with privacy regulations requiring purpose specification.

- **Permission and Transparency - Unawareness, Non-compliance (Consent)**

Informing consumers and offering opt-in/opt-out empowers them and ensures consent-based processing where required.

- **Access Management - Disclosure of Information, Non-compliance (Legitimate Interest)**

Role-based access and authentication minimize exposure and unauthorized disclosure, aligning with the organization's legitimate interest in securing data.

- **Data Security Measures - Disclosure of Information, Detectability (Legal Obligation)**

Encrypting purchase and payment information and enforcing breach-prevention measures satisfy legal duties under privacy and cybersecurity laws.

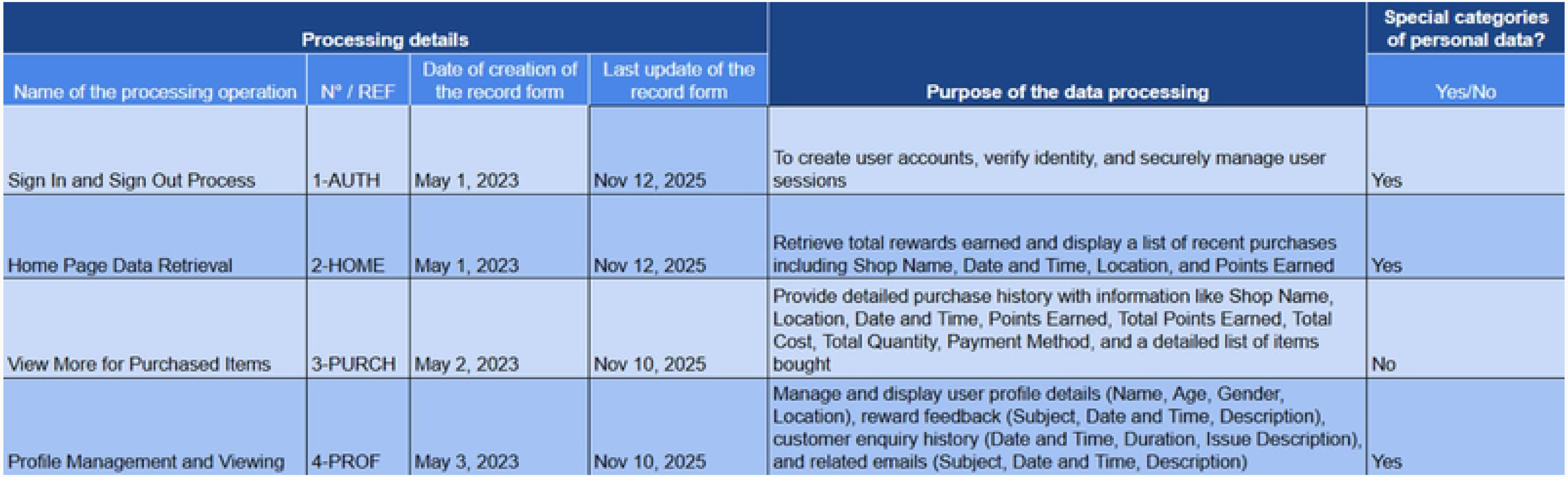
- **Frequent Privacy Audits - Non-compliance, Disclosure of Information (Legal Obligation)**

Regularly reviewing retention, third-party risks, and GDPR/CCPA compliance prevents regulatory non-compliance and limits risk of improper disclosure.

Further Privacy by Design Activities

LINDDUN Category	Threat	PbD Actions
Linking	Same customer’s actions can be joined into a profile.	Use random/pseudo IDs,limit shared data, separate data.
Identifying	Data like age + location can identify a person.	Remove or hide details, group values,add noise in reports.
Non-repudiation	Logs can prove a specific user did an action.	Use anonymous/rotating IDs,keep only summary logs.
Detection	Others can see when a user is active in the system.	Encrypt traffic,add padding/batching to hide patterns.
Information Disclosure	Personal and purchase data might leak or be misused.	Encrypt data,strict access rights,secure APIs. AES-256
Unawareness	Customers don’t know what data is collected or why.	Clear notices,consent options,simple privacy dashboard.
Non-compliance	Rules like GDPR/CCPA are not fully followed.	Short retention,delete on request,regular privacy checks.

Compliance and Conclusion



Processing details					Special categories of personal data?
Name of the processing operation	Nº / REF	Date of creation of the record form	Last update of the record form	Purpose of the data processing	Yes/No
Sign In and Sign Out Process	1-AUTH	May 1, 2023	Nov 12, 2025	To create user accounts, verify identity, and securely manage user sessions	Yes
Home Page Data Retrieval	2-HOME	May 1, 2023	Nov 12, 2025	Retrieve total rewards earned and display a list of recent purchases including Shop Name, Date and Time, Location, and Points Earned	Yes
View More for Purchased Items	3-PURCH	May 2, 2023	Nov 10, 2025	Provide detailed purchase history with information like Shop Name, Location, Date and Time, Points Earned, Total Points Earned, Total Cost, Total Quantity, Payment Method, and a detailed list of items bought	No
Profile Management and Viewing	4-PROF	May 3, 2023	Nov 10, 2025	Manage and display user profile details (Name, Age, Gender, Location), reward feedback (Subject, Date and Time, Description), customer enquiry history (Date and Time, Duration, Issue Description), and related emails (Subject, Date and Time, Description)	Yes

ShopSmart embeds **GDPR compliance** into both its app and backend through clear consent controls, strong user control and **strict data minimisation.** With transparent options **DPO-led auditing** and a **Privacy-by-Design architecture**, it processes only necessary data while maintaining accountability and customer trust.