DAYANANDA SAGAR COLLEGE OF ENGINEERING
An Autonomous Institute Affiliated to VTU, Belagavi Approved by AICTE ; ISO 9001:2015 Certified
Accredited by National Assessment Accreditation Council (NAAC) with 'A' grade
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Artificial Intelligence & Machine Learning

Incident Identification		
Submitted By: Priya Sharma	**Date & Time:**28 Oct 2025, 10:30 AM	**Report Ref No:**DSCE/AIML/IR/2025-01
Title: Customer Data Breach in Online Retail Platform	**Company:**ShopSmart Pvt. Ltd.	**System / Application:**Customer Management System (CMS)

Type of Incident Detected					
Denial of Service		**Malicious Code**		**Unauthorized Use**	✓
Unauthorized Access		**Unplanned**		**Other**	

Description

On 26 October 2025, the company's cloud database was found to be publicly accessible due to a misconfigured storage bucket. The exposed data contained names, email IDs, and addresses of 25,000 customers. The breach was identified by a security analyst after observing abnormal API calls to the CMS server.

This incident constitutes a personal data breach under **GDPR Article 33** and a personal data processing failure under **Section 8(5) of the DPDP Act, 2023**.

People Involved

- Data Protection Officer – Mr. Rajesh Verma
- Security Engineer – Ms. Kavya Nair
- IT Administrator – Mr. Suresh Kumar
- External Cloud Vendor – CloudX India Pvt. Ltd.

Others Notified

- Company Management Board
- Customers via email notification
- Data Protection Authority (GDPR)
- Data Protection Board of India (DPDP Act)

Actions

Identification / Verification measures: Security audit logs analyzed; API access from unauthorized IPs

identified.
Containment measures: Cloud storage permissions immediately restricted; keys rotated; breached bucket closed.
Evidence collected (system logs etc.) System logs, timestamped access records, and server configuration files.
Eradication measures: Removed exposed API endpoints; revoked all public access tokens.
Recovery measures: Rebuilt secure storage with encryption and strict IAM (Identity Access Management) rules.
Other mitigation measures: Implemented automatic access monitoring and employee data privacy training.
Learning: Regular audits and secure configuration of cloud assets are mandatory. Both **GDPR** and **DPDP** emphasize *"Data by Design & Default"* — meaning privacy must be ensured from the start of system design.