PHUMELELE PEARL MLOTSHWA

28/12/2025

PREPARED BY: PEARL MLOTSHWA – BICT GRADUATE

POPIA Compliance & Cybersecurity Risk Assessment

Case Study: Mr Price – Online Retail Platform (Academic Portfolio Project)

1. Executive Summary

The assessment was conducted using publicly available information and industry-aligned cybersecurity practices. These findings are intended to demonstrate an awareness of data protection principles, risk-based analysis, and compliance considerations relevant to entry-level cybersecurity and governance, risk, and compliance (GRC) roles.

This report provides a structured POPIA-aligned privacy and cybersecurity assessment of Mr Price's online retail platform. The objective of the assessment is to identify areas in which personal information may be vulnerable to cyber or privacy threats in a typical e-commerce context, as well as to recommend achievable security solutions that are aligned with the Protection of Personal Information Act (POPIA).

2. Scope and Methodology

The methodology applied included identification of personal information processed, high-level data flow analysis, risk identification and rating, and mapping of observed risks to relevant POPIA conditions. This approach reflects common practices used in entry-level governance, risk, and compliance (GRC) assessments.

The scope of this assessment is limited to the Mr Price online retail platform, including customer account registration, online purchasing, payment processing via third-party service providers, and delivery coordination. Physical retail operations and internal human resource systems were excluded from this review.

3. Organisation Overview

Mr Price is a South African-based retail organisation offering clothing and homeware products through both physical stores and an online retail platform. The online platform enables customers to create accounts, place orders, process payments, and arrange product delivery. Due to the volume of personal information processed in this environment, effective data protection and cybersecurity controls are essential to support POPIA compliance.

4. Personal Information Identified

The following categories of personal information are processed within the online retail environment:

Data Subject	Personal Information
Customers	Full name, email address, phone number, delivery address, login credentials
Payment Information	Card details processed via third-party payment gateway
Employees	Customer service system login credentials
Third Parties	Courier contact and delivery details

5. Data Flow Description

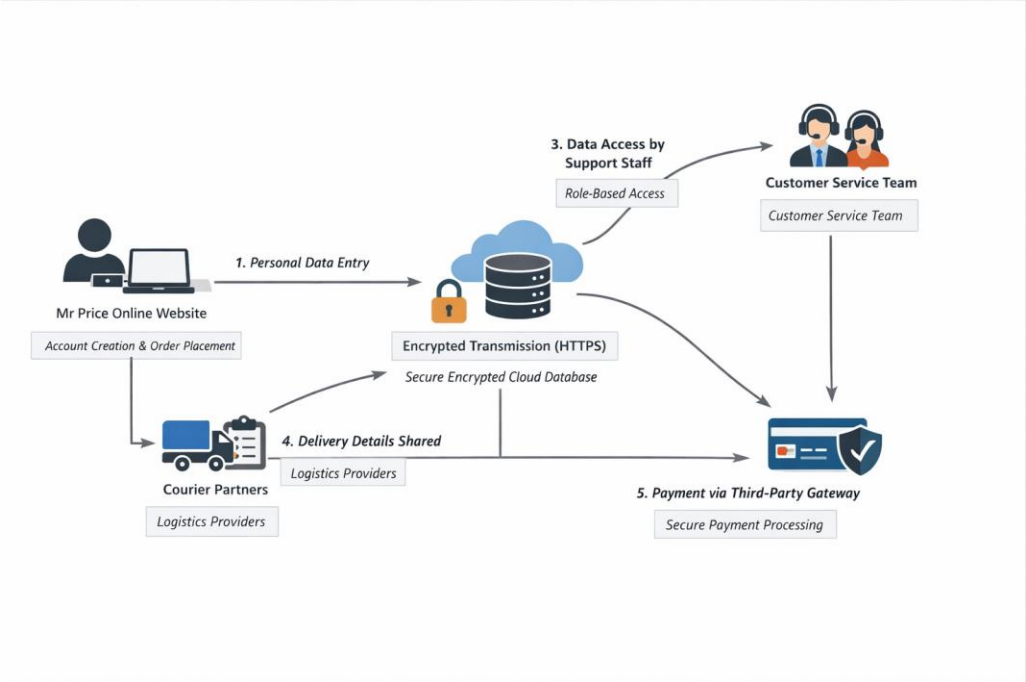
A high-level data flow review was conducted to understand how personal information is collected, transmitted, stored, accessed, and shared within the online retail environment. This review assists in identifying potential areas of exposure and informs them about the subsequent risk analysis.

5.1 Data Flow Diagram (Textual Representation)

Customer
↓ (Account registration / Order placement)
Mr Price Online Website (HTTPS Encrypted)
↓
Cloud Application Servers
↓
Customer & Order Databases (Encrypted at Rest)
↓ (Role-Based Access)
Customer Service & Operations Staff
↓
Courier / Logistics Partner

Separate Payment Flow:
Customer → Secure Third-Party Payment Gateway → Transaction Confirmation → Mr Price Online Platform

The diagram below provides a simplified representation of personal information flow within the Mr Price online retail platform:



6. Risk Identification and Analysis

Potential cybersecurity and privacy risks associated with online retail operations were identified and analysed.

Risk	Description	Likelihood	Impact
Data Breach	Exploitation of web application vulnerabilities	Medium	High
Phishing Attacks	Credential theft through social engineering	High	Medium
Insider Misuse	Unauthorised employee access	Low	High
Third-Party Breach	Courier or payment provider compromise	Medium	High

7. POPIA Compliance Mapping

The assessment focused on key POPIA conditions relevant to online retail operations, including Accountability, Purpose Specification, Security Safeguards, Openness, and Data Subject Participation.

8. Security Control Recommendations

Technical Controls:

- HTTPS/TLS encryption
- Multi-factor authentication for administrative users
- Database encryption at rest
- Web Application Firewall
- Centralised logging and monitoring

Organisational Controls:

- POPIA awareness and training programmes
- Access control and password policies
- Third-party data processing agreements
- Regular cybersecurity risk assessments
- Documented incident response procedures

9. Incident Response and Breach Notification

In the event of a data breach, the organisation should identify and contain the incident, assess the impact, notify the Information Regulator and affected data subjects as required by POPIA Section 22, and document corrective actions.

10. Conclusion and Ethical Disclaimer

This assessment demonstrates how POPIA principles can be applied within an online retail environment. The findings and recommendations are based on hypothetical risks and publicly available information. This report does not represent real vulnerabilities or internal processes of Mr Price.