# Data Breach Incident of Adastria Asia Co., Limited
# Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

## Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by Adastria Asia Co., Limited (Adastria).

The investigation arose from a data breach notification submitted by Adastria to the PCPD on 18 November 2024, reporting that its customer relationship management platform and e-commerce platform (collectively, the Affected Platforms) were accessed by an unauthorised third party, which resulted in the exfiltration of the personal data of Adastria's customers (Incident).

The investigation revealed that the Affected Platforms operated as a Software-as-a-Service (SaaS) which was provided by a third-party vendor (the Platform Vendor). In the Incident, the threat actor used the credentials of an administrator account of a current employee to connect to the Affected Platforms from an unknown overseas IP address and downloaded the order information stored therein.

Adastria is a Japanese multinational corporation engaging in fashion retail in various Asian countries. At the time of the Incident, Adastria was managing the sales of its affiliated brands (including GLOBAL WORK, "niko and …", LOWRYS FARM, Heather, JEANASiS, studio CLIP, repipi armario, LEPSIM, PAGEBOY) in Hong Kong through its online platform "dot st HK". The personal data of a total of 59,205 customers was affected by the Incident. The personal data affected included the names, telephone numbers and order information of customers (including the transaction reference numbers, order dates, membership numbers, delivery methods, deliver/pickup dates, delivery addresses, product names and descriptions, and price information).

During the course of investigation, Adastria discovered that the affected personal data was disclosed in the Dark Web approximately two months after the Incident and was made available for download.

Adastria notified all affected customers after the Incident. Adastria also implemented various remedial measures to address the deficiencies identified in the Incident, including enabling the security functions of the Affected Platforms, such as password measures, multi-factor authentication and IP address restriction function, and deploying an endpoint detection and response solution to detect and block any malicious activities on its information systems.

## Investigation Findings

The PCPD conducted five rounds of inquiries and reviewed the information provided by Adastria in relation to the Incident, including two investigation reports provided by a third-party consultant engaged by Adastria, and the follow-up and remedial actions taken by Adastria after the Incident. Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of Adastria contributed to the occurrence of the Incident (See Annex 1 for details):-

1. Weak password management;
2. Failure to enable multi-factor authentication for access to accounts;
3. Lack of awareness to ensure the security of personal data; and
4. Failure to conduct proper security reviews on the Affected Platforms.

## The Privacy Commissioner's Decision

Given that Adastria is a well-known multinational fashion brand group and holds a large volume of the personal data of customers, the Privacy Commissioner regretted to note Adastria's lack of awareness in data security and the absence of proper measures to protect the personal data in its possession. The Privacy Commissioner was of the view that had Adastria adopted appropriate and adequate organisational and technical security measures before the incident, the Incident could likely have been avoided.

Based on the above, the Privacy Commissioner found that Adastria had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening Data Protection Principle 4(1) of the Personal Data (Privacy) Ordinance concerning the security of personal data.

The Privacy Commissioner has served an Enforcement Notice on Adastria, directing it to take measures to remedy the contravention and prevent recurrence of similar contraventions in the future.

## Recommendations

Through this report, the Privacy Commissioner recommends organisations to adopt appropriate organisational and technical measures to safeguard their information systems that contain personal data so as to strengthen data security:

- Establish clear internal policies and procedures to safeguard the security of information systems and ensure thorough implementation of the same;
- Implement effective measures to prevent, detect and respond to cyberattacks, including conducting regular vulnerability scans and patching cybersecurity vulnerabilities in a timely manner;
- Cease the use of end-of-support software and upgrade software in a timely manner;
- Enhance password management of information systems and adopt multi-factor authentication;
- Conduct comprehensive security risk reviews and audits for information systems regularly;
- Configure appropriate security functions on service platforms provided by third-party vendors and conduct regular security review;
- Formulate a data breach response plan; and
- Provide appropriate training to employees to improve their data security awareness.

**Ada CHUNG Lai-ling**
**Privacy Commissioner for Personal Data**
**21 August 2025**

**Annex 1**

# Data Breach Incident of Adastria Asia Co., Limited
# Deficiencies that Contributed to the Incident

1. **Weak password management**: The passwords for all users of the Affected Platforms consisted of simple six-digit password combinations and had remained unchanged for two years before the Incident. Despite various password management measures applicable to the Affected Platforms were provided by the Platform Vendor, including setting the minimum length and complexity of password, auto-expiration of password, as well as the function of account lockout after repeated failed login attempts, Adastria did not configure these readily available password management measures;

2. **Failure to enable multi-factor authentication (MFA) for access to accounts**: While MFA was a readily available security function of the Affected Platforms offered by the Platform Vendor, Adastria did not enable MFA for all user accounts at the time of the Incident, including the administrator account that was compromised;

3. **Lack of awareness to ensure the security of personal data**: The Platform Vendor provided a range of security features for the Affected Platforms, including password management measures, MFA function, monitoring login function and IP address restriction function. However, Adastria did not enable any of these security measures at the time of the Incident; and

4. **Failure to conduct proper security reviews on the Affected Platforms**: Although the Platform Vendor would conduct regular security reviews of the infrastructure of the Affected Platforms, Adastria failed to conduct any security reviews from the perspective of a service user before the Incident.