October 23, 2026

To whom it may concern

Company Name: XEBIO HOLDINGS CO., LTD.

Representative: Tomoyoshi Morohashi, President and Representative Director

Securities Code: 8281; Tokyo Stock Exchange Prime Market

Contact: Kenji Tamura, Executive Officer, XEBIO CORPORATE CO., LTD.

(Tel: +81-3-6870-6008)

Notice Concerning the Potential Leakage of Personal Information of a Consolidated Subsidiary Due to Unauthorized Access to an E-Commerce Platform Operated by a Third Party

XEBIO HOLDINGS CO., LTD. (the "Company") hereby announces that unauthorized access occurred on an e-commerce platform operated by a third party, and that customers' personal information of GALLERY・2 Co., Ltd. (the "Subsidiary"), a consolidated subsidiary of the Company that used the platform, may have been leaked to external parties. The Company hereby provides the following information based on the findings confirmed as of the date of this announcement.

We sincerely apologize to our customers and all other parties concerned for the considerable concern and inconvenience caused by this incident.

1. Overview of the Incident

Unauthorized access by a third party occurred on "Commerble," the e-commerce platform used by the Subsidiary.

According to a report received from Sigma Consulting Co., Ltd., the parent company of Commerble Co., Ltd., the operator of the platform, authentication credentials used for system administration by Commerble Co., Ltd. were illegally obtained on October 16, 2026. On October 17, unauthorized access to the Subsidiary's customer database was carried out through the platform's administrative cloud environment, and operations to display customer information were confirmed.

Furthermore, on October 18, tampering with the payment information entry screen of the e-commerce website was detected, and the website was suspended on the same day.

According to the report, improperly configured access restrictions and other security settings in the system were exploited. Commerble Co., Ltd. and Sigma Consulting Co., Ltd. are continuing their investigation into the specific cause of the intrusion and the extent of any information leakage.

2. Personal Information Potentially Affected

The personal information that may have been leaked is as follows:

Category	Number of Records	Details
(1) Purchaser Information	Up to approximately 128,000	Purchaser names and email addresses (excluding duplicates)
(2) Address Information	Up to approximately 122,000	Purchaser addresses, shipping addresses, and telephone numbers (excluding duplicates)
(3) Email Transmission History	Up to approximately 158,000	Order confirmation email contents and recipient email addresses

There is overlap among these categories, and the sum of the above figures does not represent the number of individuals whose personal information may have been affected.

It has been confirmed that operations to display the relevant information in the customer database were performed through unauthorized access. However, as of the date of this announcement, there is no confirmed evidence that the information was extracted or transferred outside the system.

The information concerned does not include credit card numbers or login passwords.

As of the date of this announcement, no specific secondary damage, such as misuse of personal information or financial losses resulting from this incident, has been confirmed.

3. Status of Response

The Subsidiary suspended its e-commerce website on October 18, 2026.

Commerble Co., Ltd., the operator of the e-commerce platform, and its parent company, Sigma Consulting Co., Ltd., have reported that they have implemented measures to prevent further damage, including disabling external access to administrative functions, changing authentication credentials and connection information, correcting access restrictions, and reviewing access privileges.

In addition, the Subsidiary submitted a report concerning this incident to the Personal Information Protection Commission of Japan on October 21, 2026.

4. Notification to Customers and Contact Information

The Subsidiary is preparing individual notifications and precautionary notices for potentially affected customers, taking into account the progress of the investigation.

For inquiries regarding this incident, please contact the following:

Contact: G2 Security Desk
Email: security@gallery2.jp

Customers are advised not to access links or enter personal or payment information if they receive suspicious emails or other communications impersonating the Subsidiary.

5. Future Measures and Prevention of Recurrence

Based on the findings of investigations by external specialists and other relevant parties, the necessity of additional security measures will be assessed.

The Subsidiary will consider gradually resuming operation of its e-commerce website after confirming its security.

The Company Group will also review its management and oversight framework for external cloud services and take measures to prevent similar incidents from recurring.

6. Impact on Financial Results

The impact of this incident on the consolidated financial results of the Company Group is expected to be immaterial.

Should it become apparent that this incident will have a material impact on the Company's financial results, or should any other matters requiring disclosure arise, the Company will promptly make an announcement.

End

Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.