May 31, 2024

For immediate release

Company Name:	kaonavi, inc.
Representative:	Hiroyuki Sato Representative Director, President & Co-CEO
Code:	4435 (TSE Growth)
Inquiries:	Kimitaka Hashimoto Director & CFO
Email:	ir@kaonavi.jp

(Progress Regarding Disclosed Matters) Notice Regarding Results of Investigation of Personal Data Leakage at a Subsidiary and Measures to Prevent Recurrence

As stated in our release "Notice and Apology Regarding Leak of Personal Information at a Subsidiary" dated March 29, 2024, our subsidiary, Work Style Tech Ltd. ("WST"), discovered that the personal data of its customers was accessible from the outside under limited specific conditions and that some of that personal data was leaked.

We hereby announce that the investigation of this matter has been completed and that measures to prevent recurrence were formulated, as stated in the attachment. (The attachment is a press release by WST.)

We sincerely apologize to all our customers and all relevant parties for any inconvenience or concern this may have caused. We will continue to encourage our group companies to improve security and to strictly manage data, including personal information.

At this time, we have made no changes to the financial forecast related to this incident. Should there be any facts to be disclosed in the future, we will disclose them in a timely manner.

[Translation]

May 31, 2024

To: All customers

Work Style Tech Ltd.

Apology Regarding Personal Data Leakage and Announcement on Measures to Prevent Recurrence

As stated in our release "Important Notice and Apology to Customers Using Our Service" on March 29, 2024, it was discovered that there was a leakage of our customer's personal data in our service "WelcomeHR" (the "Incident"). Once again, we sincerely apologize to our customers and all concerned parties for any inconvenience or concern this may have caused.

We take this situation very seriously and will strengthen the personal information management system and thoroughly educate employees to prevent recurrence. Through these measures, we will do our utmost to regain trust from our customers and concerned parties. Also, we have yet to find the fact that any personal data leaked due to the Incident has been misused or that customers have suffered from any secondary damage to date. However, we will continue relevant investigations and efforts to prevent secondary damage.

We would like to inform you of the results of the investigation concerning the Incident which we have conducted to date and efforts to prevent recurrence.

1. Overview of the Incident

Due to incorrect setting of access authorizations for our cloud storage, data files that customers uploaded through our service were made available for external access under specific conditions* during the period from January 5, 2020 to March 22, 2024 (the "Duration"). And, in fact, it was discovered that a third party had downloaded files by unauthorized access during the period from December 28, 2023 to December 29, 2023.

Unauthorized access was made to the environment containing information on customers who have agreements directly with us. Data of customers under OEM agreements or sub-license agreements was not accessed or leaked.

*Files were not in a condition that any one could access them but in a condition that they could be accessed and downloaded if specific operations were performed.

2. Course of Events for the Incident

March 22, 2024: During the course of security investigation, the incorrect setting of access authorizations to cloud storage was detected. This incorrect setting was immediately corrected on the same day.

March 28, 2024: As a result of a follow-up investigation, it was confirmed that there were traces of files on the cloud storage having been downloaded by a third party's unauthorized access.

March 29, 2024: We announced the Incident on our website. Also, we submitted a breach report (prompt report) to the Personal Information Protection Commission (the "PPC") in accordance with the Act on the Protection of Personal Information of Japan (the

"APPI") and consulted with the police station. From the same day to April 26, we informed the corporate customers with whom we have contracts. For end users, we established a customer consultation desk and started to inform end users of the leaked data by individual notices or public announcements on a step-by-step basis. We are still responding to inquiries from our customers.

April 11, 2024: We asked an external specialized organization for dark web investigation concerning secondary damage. The investigation is still ongoing.

April 26, 2024: The external specialized organization reviewed server settings, and issues they pointed out which might lead to information leakage were immediately rectified to secure safety on the same day. Also, we developed a plan to rectify other minor issues with no risk of information leakage, and they are being rectified on a step-by-step basis.

May 24, 2024: We submitted another breach report (the definitive report) to the PPC in accordance with the APPI.

May 31, 2024: We provided additional information to the PPC.

3. Impact of the Incident

The personal data that was confirmed to have been leaked as a result of the Incident consists of PDF files and image files, such as various identification cards, that customers uploaded to the cloud storage through our service during the Duration (i.e., names, postal addresses, dates of birth, sex, phone numbers, etc. contained in those files). The number of end users (customers) related to such data is as follows:

We individually informed each corporate customer and end user with whom we have contracts and whose information was leaked on a step-by-step basis.

Total number of end users whose personal data was leaked: 158,929

(1) Of the total number above, number of end users whose personal data was downloaded by a third party: 150,445

(2) Of the total number above, number of end users whose My Number information (*kojinbangoujyouhou*) was included: 46,329

(3) Of the total number above, number of end users whose credit card or debit card information was included: 8,073

(4) Of the total number above, number of end users whose Special Care-Required Personal Information (*youhairyokojinjyouhou*) was included: 2,707

  (i) Of the number in (4) above, number of end users whose health checkup information was included: 1,937

  (ii) Of the number in (4) above, number of end users whose disability information was included: 798

The customers with whom we have directly agreements were affected by information leakage due to the Incident. There is no data leakage or other effects for customers under OEM agreements or sub-license agreements.

4. Secondary Damage

We and the external specialized organization conducted the investigation and do not confirm that any personal data that was leaked due to the Incident has been misused to date.

5. Cause

The cause is that files that customers uploaded through our service had been available for external access and download under the specific conditions, due to incorrect setting of access authorizations to the cloud storage where files containing customers' personal data are stored.

6. Measures to Prevent Recurrence

As stated in Section 2 above, the incorrect setting of access authorizations to cloud storage was corrected on March 22, 2024.
In addition, based on the above, we will implement the following measures to prevent recurrence (including those completed).

(1) Enhancement of system management structure

We will establish a double-check system for designing and modifying cloud settings to strengthen our monitor system so that we can respond immediately when any unauthorized access or other abnormality occurs.

Should any unauthorized access occur, as measures to prevent further damage, we will separate storage locations for files we received from each customer and make access restriction controls stricter.

We will work with the external specialized organization for the management system and security measures as mentioned above and will review and improve them on a regular basis.

(2) Enhancement of vulnerability assessment

In order to check any deficiency other than the incorrect setting of access authorizations to cloud storage which caused the Incident, we asked the external specialized organization for an assessment of cloud settings on April 26, 2024, and issues they pointed out which might lead to information leakage were immediately rectified to secure safety on the same day. Also, we developed a plan to rectify other minor issues with no risk of information leakage, and they are being rectified on a step-by-step basis.

In addition to regular vulnerability assessment for applications and networks which are currently carried out, we will perform the above-mentioned cloud setting assessment on a regular basis.

(3) Re-education on information security for employees

We will work with the external specialized organization and re-educate employees regarding personal information protection and information security.

Once again, we sincerely apologize to our customers and all concerned parties for a great inconvenience or concern this may have caused.

As a business operator handling customers' important personal information, we take this situation very seriously and will do our utmost to prevent recurrence. Also, we will do our best to regain trust from our customers and concerned parties.

Contact for inquiry for the Incident:
Work Style Tech Ltd.
E-mail: support@workstyletech.com