March 29, 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

Notice and Apology Regarding Leak of Personal Information at a Subsidiary

Our subsidiary, Work Style Tech Ltd. ("WST"), has discovered that the personal information of its customers was accessible from the outside under certain limited conditions and that some of this information had been leaked.

The above situation has already been corrected, and there is no risk of leakage at this time. The details of the currently known facts are described in the attached 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, although the impact on the business results is under scrutiny. Should there be any facts to be disclosed in the future, we will disclose them in a timely manner.

[Translation]

March 29, 2024

To: All customers

Work Style Tech Ltd.

Important Notice and Apology to Customers Using Our Service

It has recently been discovered that in our company's "WelcomeHR" service ("Our Service"), personal data of our company's customers was accessible from the outside under certain limited conditions, and personal data was leaked as a result (the "Incident"). We hereby inform you of the details thereof and the current situation as follows.

We sincerely apologize for any concerns this may cause.

1. Outline of the Incident

Originally, the list of files stored by customers on the storage server should not have been accessible from the outside, but it was accessible due to misconfiguration of access authority for that server.

It was found that due to such misconfiguration, each file was also available for download based on the information in the list of files and that files were actually downloaded by a third party.

2. Items of leaked personal data and number of affected individuals

Items of personal data:

Names, genders, addresses, phone numbers, various identification cards uploaded by customers (Individual Number Cards (My Number Cards), driver's licenses, passports, etc.), and images of resumes and the like

Number of affected individuals

162,830 persons (of these, the number of persons whose data was confirmed to have been downloaded is 154,650)

The information leaked in the Incident originated from the environment of customers with whom our company has direct contracts. Since customers using our Service under OEM agreements or sublicense agreements operate in a different environment, they are not affected by the Incident.

3. Period

i. Period during which it was confirmed that personal data had been downloaded:
December 28, 2023 to December 29, 2023

ii. Period during which personal data was accessible from the outside:
January 5, 2020 to March 22, 2024

4. Cause

Misconfiguration of server access authority.

5. Background

During a security investigation carried out on March 22, 2024, it was reported that there was a misconfiguration of server access authority. On the same day, our company immediately fixed the configuration. As a result of an investigation thereafter, on March 28, 2024, it was found that a third party had downloaded information during the above period.

6. Existence and details of secondary damage or possibility thereof

Although the investigation is still ongoing, at present, we have not found any occurrence of secondary damage.

7. Current situation

We have conducted an inspection, and the access authority for files on the storage server has been changed to an appropriate configuration; therefore, currently no files are accessible from the outside.

In addition, we have separately contacted the business operators whose information had been leaked.

8. Measures to prevent recurrence

We take this matter seriously and will make efforts to prevent recurrence of similar incidents, such as by providing employees with thorough training and establishing a system to continuously monitor server configurations.

Point of contact for the Incident:

Work Style Tech Ltd.
Contact address: support@workstyletech.com