October 25, 2023

Supplemental Information regarding compromise on FENICS (Philippines)

On March 17, 2023, Kyocera Corporation issued a public notice that the FENICS Internet service, which was provided by Fujitsu Limited (hereafter "Fujitsu") to Kyocera Corporation and some of the group companies, had been compromised. Kyocera Circuit Design Philippines, Inc. (hereafter “KCDPH”) is among the group companies that had been affected. Kyocera Corporation’s public notice is accessible here: https://global.kyocera.com/newsroom/information/2023/03/information-regarding-compromise-on-fenics.html

Please refer below for details published by Fujitsu regarding the incident: https://www.fujitsu.com/jp/services/infrastructure/network/news/2023/0220.html (in Japanese)

Due to this incident, unknown third parties were possibly able to access data from the Fujitsu system which may include email addresses, users' names, and other data included in emails of those transacting with KCDPH from the period of March 28, 2022 to May 15, 2022 (the “Email Data”).

The final investigation conducted by Fujitsu resulted in the replacement of identified compromised network devices, but it could not conclusively identify the inclusion of compromised data sent in and out from KCDPH users. At the same time, KCDPH has not confirmed if any third parties have illegitimately used the affected Email Data.

We sincerely apologize to those who may worry about this matter. We will further strengthen information security measurements in a bid to minimize, if not altogether avoid, this situation from happening again. In this regard KCDPH has:

1. Notified the National Privacy Commission and identified data subjects of the incident;
2. Switched the email service provider from Fujitsu to a new service provider. The security enhancement measures implemented by the new service provider include:
    (i) introducing multi-factor authentication when users log into their email accounts.

(ii) enforcing access restrictions that allow users to access Kyocera environments only from within the company (example: no access from users' home PCs).
(iii) checking email attachments for malicious content.
(iv) scanning URL links in messages in the body of email to protect users from connections to dangerous links.

3. Implemented the measures to enhance information security through its IT section, including:
   (i) Requiring employees to use strong passwords with at least 8 alphanumeric characters and special characters for email accounts and resetting the password at least twice a year.
   (ii) Installing anti-virus software to scan and block spam emails and unwanted or unknown sender emails.
   (iii) Disallowing employees to access their personal emails using company equipment and facilities.
   (iv) Restricting employees' access to certain blocked websites and requiring permission of administrator if access is required.
   (v) Providing training to educate all employees about email security risks and best practices.
   (vi) Frequently reminding all employees to be wary about unusual or suspicious emails and to avoid clicking on suspicious links or downloading attachments from such emails.

In order to reduce any harm or negative consequences that may result from this security incident, KCDPH has notified identified data subjects and have asked them to: (i) change their passwords, (ii) notify KCDPH if they notice any suspicious activity, and (iii) ignore and refrain from opening e-mails coming from unknown sender.

For further information, please contact our Data Protection Officer through: dpophreport@gp.kyocera.jp.

If you require any assistance in relation to the incident, please contact us through https://contact.kyocera.co.jp/inquiry/gl/others/input.html.

(Please enter "FENICS" in the subject line of your inquiry)