

June 3, 2025

Regarding the leakage of personal information due to unauthorized access at a Group company
and the results of the investigation (third report)

Zeon Corporation
Tohpe Corporation

As announced on our website in March 2025, Tohpe Corporation (Tohpe), a Group company of Zeon Corporation (Zeon), experienced unauthorized access to part of its servers by a third party, and the possibility that personal information was leaked has been identified. While no misuse of that information has been confirmed to date, we sincerely apologize for the considerable concern and inconvenience caused to all affected parties.

Following our previous update, we continued our internal investigation in parallel with an independent review conducted by an external investigative agency. These investigations have now concluded, and we hereby report the findings as follows.

1. Investigation details and findings

The external investigative agency examined the log files and server status data from the Tohpe servers affected by the unauthorized access. The agency identified the incident, determined the scope of its impact, and specified the data that serves as evidence. As a result, traces of personal information leakage were discovered, and it was confirmed that this data had at one point been downloadable from certain external websites. At present, the relevant data is no longer publicly available on those websites, and it has been confirmed that it cannot be downloaded.

2. Personal information confirmed to have been leaked externally (20,161 records)

(1) Customer information managed by Tohpe (19,583 records)

Category	Leaked information	Records
Tohpe product business partner representatives	Full or partial details of the following: Representative’s name (or surname only), company name, company address, company phone and fax numbers, department, and position	1,277
Customers involved in the purchase, sale, or delivery of Tohpe products or those who used Tohpe products	Full or partial details of the following: Customer’s name (or surname only), company name, company address, company phone and fax numbers, department, position	18,019
Building owners at sites where Tohpe paint products were delivered	Owner’s name (or surname only), construction site address	287

(2) Account information of Tohpe employees and former employees (578 records)

Full or partial details of the following:

• User ID issued by Tohpe	• Email address issued by Tohpe	• Name (kanji and kana)
• Department name	• Organization code	• Employee number
• Phone number	• Address	• Date of birth
• Date of joining and resignation		

The above personal information may be misused for unsolicited phone calls, spam emails, or phishing scams. If any suspicious emails or other communications are received, please contact Tohpe’s Personal Information Inquiry Desk, whose phone number is provided at the end of this notice.

3. Status of measures taken

(1) Interim measures

In coordination with the external investigative agency, we conducted a forensic investigation to check for signs of intrusion in all servers, data, PCs, and network devices. We ensured firewall safety, restricted server access, implemented partial email restrictions, temporarily suspended website access, and limited the use of external connections.

(2) Permanent measures

We are enhancing endpoint security on PCs through the introduction of EDR, upgrading and strengthening firewall security, partially restricting international access, enforcing stricter internal access controls, and improving security monitoring. Furthermore, we will continue conducting regular employee training on information security and will strengthen internal systems by updating cybersecurity policies, expanding employee education, and reinforcing our IT governance structure.

4. Operational status of Tohpe's systems

Tohpe's systems, which were temporarily shut down due to a system failure, resumed operations by May 9, 2025, after confirming system safety. Tohpe's website also resumed operations as of May 22, 2025, with certain services still unavailable. We sincerely apologize for the inconvenience caused during the suspension period.

Please note that Tohpe's servers and networks operate independently from those of Zeon and other Zeon Group companies. No impact related to this incident has been confirmed at any other Group companies.

5. Response by Zeon and Tohpe

(1) Response to individuals whose personal information was leaked

Starting June 3, 2025, Tohpe is sending letters of apology and explanation to affected individuals. For those whom we cannot contact directly, this public notice serves as formal notification.

(2) Reports to authorities

Tohpe submitted an initial report to the Personal Information Protection Commission of Japan promptly after discovering the incident and submitted a formal follow-up report on April 25, 2025, based on the findings of the external investigation. Zeon also reported the incident to the Ministry of Economy, Trade and Industry, and Tohpe notified the Osaka Prefectural Police Headquarters on March 13, 2025. We will fully cooperate with any future investigations.

Zeon and Tohpe take this incident very seriously. With the cooperation of external experts, we are committed to further strengthening our information security systems and implementing thorough preventive measures.

For previous updates on this matter, please refer to [the first report](#) dated March 14, 2025, and titled "Notice of system disruption due to unauthorized access at a Zeon Group company," as well as [the follow-up notice](#) dated March 19, 2025.

Should any new developments arise, we will provide prompt updates.

Inquiries regarding this matter

For inquiries related to personal information: Contact Tohpe Corporation's Personal Information Inquiry Desk by phone (+81-72-243-6410) (Hours: 9:00–17:00)

For media inquiries: Contact the Department of Corporate Communications, Corporate Sustainability Division, Zeon Corporation by phone (+81-3-3216-2747) or via the [Contact Form](#)