



European School Luxembourg I

Personal data breach:
Document on external communication
to relevant persons

DOCUMENT ON EXTERNAL COMMUNICATION OF A PERSONAL DATA BREACH TO RELEVANT PERSONS



DATA BREACH NOTIFICATION

We are writing to you about a matter of concern related to your personal data. We are aware of the importance you place on your privacy and we take the protection of your personal data very seriously.

1. What happened?

On 09/01/2024, our IT Department discovered that a local server, which was used for certain teaching activities, had been targeted by a cyberattack.

The concerned program was identified by IT specialists during the investigation as *Moodle*. The program's local account is different from *School Management System* (SMS) and *Office365* (O365) accounts because it is stored on a local server at the school. Although active, the program's automatic process for cleaning up inactive users did not work. As a result, data about you was always recorded.

2. What information was involved?

Information related to you has been exfiltrated.

The relevant information included:

- Email address provided by the school;
- Last name;
- First name;
- Cycle and Level (for students only);
- Username.

3. Likely consequences of the personal data breach

Due to this unfortunate event, we predict that one or more of the following scenarios may take place:

- Your email addresses may be subject to mailing and/or fishing/phishing attempts. Insofar as you are no longer part of our establishment, the risk would be minimal or nonexistent. However, if it happens and to protect you, please refer to the detailed recommendations on point 5, page 3 of 3, of this document;
- Data could be deleted from the affected server. The impact would be minimal or nonexistent;



4. What are we doing?

We immediately took measures to determine the nature and the scope of the unfavorable event after it was detected. We are also collaborating with the Luxembourgish National Authority (CNPD), the Computer Incident Response Center Luxembourg (CIRCL) and the Police.

Measures to protect our community:

- Shutdown of the affected server on 09/01/2024;
- Identification and correction of the vulnerability in the attacked program;
- Deletion of your data.

5. What should you do?

In light of the circumstances and the effort taken by the European School to mitigate the situation, we believe:

☐ there is no further action for you to undertake;

☒ there is action for you to undertake :

- If you detect a suspicious email, delete it from your inbox without even opening it;
- If you receive an email that you cannot determine whether it is suspicious or not, it should be sent to your ICT Department;
- Your ICT Department will carry out a check and inform you of the action to be taken.

6. For More Information

For more information, please contact our Data Protection Officer (DPO) : LUX-DPO-CORRESPONDENT@eursc.eu

Yours sincerely,