DataClassroom PII Protection

December 21, 2021

This document describes what **Personally Identifiable Information (PII)** is collected by the DataClassroom application, and how it is protected.

It provides a short summary of details described in the **DataClassroom IT Security Strategy** document, which is available on request.

Definition of Terms

Referring to the Code of Federal Regulations, Title 34, Section 99.3, the following definitions apply:

1. *Directory Information* (means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed)
2. *Personally Identifiable Information (PII)*
3. *Education Records*
4. *Biometric Record*

Scope of PII collected

No *Education Records* or *Biometric Records* are collected by the application.

The only *PII* collected is information also designated as *Directory Information*:

1. Email address (for students, the “school” email, not a personal email address)
2. Password
3. Name (need not be full name)

Other data collected

Additional data collected while students and teachers use the app are limited to:

- Uploaded scientific datasets i.e. information to be analyzed using the app
- Uploaded documents related to the datasets such as lesson plans, answer forms etc.
- The user’s application settings and preferences
- Logging of activity / events for usage analysis purposes
- Authentication tokens and similar used for SSO and authentication
- Basic connection logging of IP addresses, connection security data such as cookies.

Data storage and backup

Production servers containing the user *PII* are located in physically secure Amazon Web Services (AWS) data centers in the United States.

In the production SQL database:

- All passwords are stored encrypted (Bcrypt).
- Data storage is encrypted with AES-256..

Database contents are backed up to AWS “S3” storage in the same datacenter as the production servers. This “at rest” data is encrypted with AWS standard AES-256 encryption.

Access protection

They are protected from electronic access by network security involving a combination of AWS Security Groups and firewalls, plus requirements for SSL encryption for any connection, and a Security Strategy designed to prevent malicious access to any computers from which connection to the data centers takes place. More detailed documentation can be provided on request.

Data transfer

Data transfer between the servers and client computers takes place exclusively using SSL-encrypted connections (HTTPS).

Incident and breach response

We have a clear plan for our response to any security-related incident, including restoration of lost data, resumption of service and communication with affected customers. More detailed documentation of the Incident Response Plan can be provided on request.

Third parties (contractors)

No third party currently has access to the DataClassroom production servers and customer data storage.

Third parties involved in application development are required to sign appropriate contracts requiring them to treat all data received confidentially and use best practices to avoid security breaches.

Employees

Employees are required to take a training course explaining the Security Strategy and their role in relation to it, and sign a document declaring that they have received such training.

Training is repeated if any significant changes are made to the Strategy.

The Strategy includes references to applicable principles of law, with reference to the New York Consolidated Laws, Education Law EDN §2d as being a typical example of such a law, explaining key concepts particularly:

1. The Parent’s Bill of Rights
2. Requirements of third-party contractors