Log Management in Mentornity

This document provides an overview of the log management practices employed by Mentornity. It outlines the types of logs generated by the system, the data stored within these logs, and the policies regarding the retention and anonymization of user data.

1. Log Types

1.1 User Activity Logs

User activity logs capture actions performed by users within the platform. These logs are essential for maintaining a record of user interactions related to features such as meeting management, meeting notes, and available time slots. The primary purpose of these logs is to support the platform's feed functionality, which provides users with a chronological overview of their activities.

- **Data Stored**: User activity logs include the user ID, details of the activity performed, and any associated data relevant to that action.
- **Storage Duration**: These logs are stored indefinitely in our database, allowing for a complete history of user actions.

1.2 Error Logs

Error logs are crucial for diagnosing and resolving issues within the platform. When an error occurs on the backend server, detailed information about the failed HTTP request is recorded. This includes data related to the nature of the error and the user ID of the individual who encountered the issue. Error logs are used primarily for debugging and improving the platform’s stability.

- **Data Stored**: Error logs contain the user ID, request method, request path, error message, and other relevant request data.
- **Storage Duration**: These logs are retained for one year to facilitate troubleshooting and support.

1.3 Server Access Logs

Server access logs document every request made to our backend server. These logs are

essential for monitoring the platform's performance and security. Each entry includes information about the request method, path, response time, response status, and user ID if the request includes authorization information.

- **Data Stored**: Server access logs include HTTP request details (method, path, response status) and the user ID if available.
- **Storage Duration**: Server access logs are stored for one year, allowing for performance analysis and security audits.

2. User Identity in the Logs

In all logs, users are identified by their user ID rather than personal information. In cases where a user opts for anonymization, all identifiable information is permanently removed from our database. As a result, even though the logs may remain, they will no longer contain any data that can be used to trace back to a specific user. This process ensures compliance with privacy standards and safeguards user confidentiality.

This documentation is intended to provide transparency regarding our log management practices and to ensure users understand how their data is handled within the platform. If you have further questions or need additional information, please contact our support team.