

GDPR Compliance Report			
Check	Description	Result	Remedy
SSH connection	Ensure that the SSH connection to the server is secure and functional.	Passed	
MySQL connection	Ensure that the system can connect to the MySQL database.	Failed	Check the database credentials and ensure the MySQL server is running. Verify the connection string.
Privacy policy	Verify that the privacy policy exists and is accessible to users.	Failed	Ensure that the privacy policy is properly loaded to the server and placed in the correct directory.
User consent	Ensure that user consent for data processing is recorded.	Failed	Implement user consent tracking using cookies or a database. Store records for user consent.
MySQL encryption	Ensure that MySQL database encryption (SSL) is enabled.	Configured	Configure SSL encryption for MySQL. Ensure the 'my.cnf' file has the correct settings.
Data retention policy	Verify that a data retention policy is in place, ensuring data is not stored indefinitely.	Failed	Create a data retention policy and implement it. Delete data as necessary. Upload it to the server. Ensure users are aware of the policy.
Data breach policy	Ensure that a data breach detection and response plan is in place.	Not Implemented	Develop a data breach response plan, including detection mechanisms and notification procedures.
Right to access	Ensure users can access their data stored in the system, if requested.	Not Implemented	Implement a GET request feature that allows users to retrieve their data.
Right to erasure	Ensure users have the ability to request the erasure of their data.	Not Implemented	Implement a DELETE request feature that allows users to request the deletion of their data, and ensure the data is properly removed from the database.
Third-party vendors	Ensure contracts with third-party vendors are in place and GDPR-compliant.	Not Implemented	Obtain GDPR-compliant contracts from third-party vendors who process user data.