# PraxCloud Security

Praxtour realizes that with the App (PraxCloud) solution, proper protection of personal data (AVG) is essential. Below is the summary of the protection measures of the PraxCloud platform.

**Current security:**

1. The overall PraxCloud includes an SSL certificate from www.praxcloud.eu . This means that all data goes through an encrypted connection. The techniques involved are the following: TLS 1.3, X25519, and AES_256_GCM. This certificate has been issued by Xolphin to Praxtour BV.

2. In addition, the Web management with CORS is set to the API (data interface) with a CSRF token, meaning that besides the Web management, no one from outside PraxCloud can send data requests.

3. After authentication of a user, via the app or web administration, each request to the server will be assigned a unique code belonging to his account. This is 16 characters long and contains random characters. This is in a separate http header. Thus, even with knowledge of the platform address it becomes very difficult to access the data.

4. The database is hidden in an isolated environment in a virtual machine on the Digital Ocean platform. It is therefore addressed internally and cannot allow any connections from the outside. This is why the API layer is built around it.

5. We minimize, generalize and obfuscate the code of the web management that is viewable through the browser to make it difficult for the potential hacker to gain insight into the processes of data requests to and from the platform.

**Future (extension) security:**

1. In addition to Username and Password, after authenticating a Username and Password to log into the web management environment, a Google Authenticator will be installed later for MFA (Multi Factor Authentication). This provides additional security in the platform.

2. Should messages be sent through the platform, blockchain will be used for extra security.

**Data obfuscation**

In the context of the AVG and the IT department not being allowed to view personal data the following:

If data obfuscation* of, for example, the email address from the institution (customer) is desired, then we will realize that. We will include this in the contract terms, so that the customer can agree to it. In this way support can be provided whereby the email address is used as communication for the system to build in e.g. 'password forgotten' functionality.

Praxtour will provide sufficient security with its PraxCloud platform to offer good resistance against hackers. Of course Praxtour will do everything possible to strive for good data security in the future.

*Data obfuscation is the encryption of data that can only be viewed by the owner of the data.