Data Management and Protection

Version: 1.0

Introduction

This document is intended for Information Architects, Security Specialists, and Privacy Managers to enable you to better understand the management and protection of data within the NoahFace environment.

Specifically, it aims to address the following questions:

- What data is stored?
- Where is it stored?
- How is it encrypted?
- How long is it retained?
- How should it be backed up?

You may also like to review our privacy policy at: http://noahface.com/privacy

If after reading this document you have further questions about data storage or privacy, we'd be pleased to answer them. Please email us as follows:

Technical Questions: support@noahface.com

Privacy Questions: privacy@noahface.com

Key Data

The key data managed in the NoahFace platform is as follows:

Data Element	Description
Global Configuration	Data such as the type of organisation, the list of sites and access points, and the selected plan.
Billing Details	Credit card details.
Access Point Configuration	Data such as the type of screen displayed, what options are available to users, how events are handled, etc.
User Details	Data such as a user's first and last name, their profile picture or avatar, and (optionally) their phone number and email address.
User Biometrics	A user's facial characteristics, as extracted from their photos.
Access Rules	The rules that define who can make use of an access point and at what times during what days of the week.
Events	The date, time, photo, and details that record a user's interaction with an access point.

Storage Options

NoahFace provides you with three data storage options as follows:

1. Local.
2. Cloud.
3. Hybrid.

You can select the data storage option you prefer from your Web login. The table below details where each element of data is stored based on your selected storage option:

Data Element	Local	Cloud	Hybrid
Global Configuration	Cloud	Cloud	Cloud
Billing Details	Stripe	Stripe	Stripe
Access Point Configuration	iPad	Cloud	Cloud
User Details	iPad	Cloud	Cloud
User Biometrics	iPad	iPad	iPad
Access Rules	iPad	Cloud	Cloud
Events	iPad	Cloud	iPad

The billing details (eg: your credit card) are not stored in NoahFace at all, but rather in our payment gateway (Stripe). This gateway is used by thousands of platforms globally for both one time and subscription billing.

Local Storage

Local storage is appropriate for smaller deployments where there is a single iPad being used. Almost all of the data is stored locally on the iPad, and it is managed through the NoahFace App.

Cloud Storage

Cloud storage is appropriate for most deployments with two or more iPads. The majority of data (ie: access point configuration, the list of users, and access rules) is stored centrally in the Cloud, and is replicated to each iPad as needed. Events are pushed from each iPad to the Cloud as they are generated, allowing you to view them centrally using a Web browser.

Hybrid Storage

Hybrid storage is similar to Cloud storage, in that the majority of data is stored centrally in the Cloud and is replicated to each iPad as needed, however, events are not pushed from each iPad to the Cloud and can only be viewed locally. You would use Hybrid storage if you were concerned about pushing events to the Cloud, or if you did not want to consume network bandwidth for each event.

Encryption

At NoahFace, we follow best practices for the encryption of data as follows:

1. All network traffic between the NoahFace App and the NoahFace Cloud server is encrypted using industry standard TLS/SSL.
2. Sensitive user identifiable information that is needed locally on the iPads (ie: passcodes and biometrics) is encrypted at rest using Apple's keychain facilities. This is important because it means if an iPad is ever stolen, this data cannot be extracted.

Data Retention

Your event data is maintained on the iPad on which it is generated for 90 days, after which time it is automatically destroyed. If you are using Cloud storage, your event data is also maintained for 90 days in our NoahFace Cloud storage. After this time, it is automatically and permanently destroyed.

If your iPad has limited storage, or you are generating an extreme number of events, events may be kept for less than 90 days on the iPad. This restriction does not apply to Cloud storage, where there is no limit to the number of events you can retain.

Backups

If you are using Local storage, we strongly recommend you backup your iPads using Apple's iCloud services. If your iPad is ever broken or stolen, you will then be able to quickly restore it to a new iPad.

If you are using Cloud storage, it is not strictly necessary to backup your iPads, as all data (with the exception of biometric data) is managed in the Cloud. If your iPad is ever broken or stolen, you will be able to connect a new iPad, and the configuration and user data will be automatically re-synchronised. However, users would need to re-regsiter on the new iPad, so if you wanted to avoid that possibility you could choose to still perform iCloud backups, perhaps less frequently.

If you are using Hybrid storage, you should also consider that events are only stored on the iPads on which they are generated. However, it is still not strictly necessary to perform backups as the loss of events would not preclude you from being operational quickly using a new iPad.