Data Management and Protection

Version: 8.12.0

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?
- How is user consent handled?

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

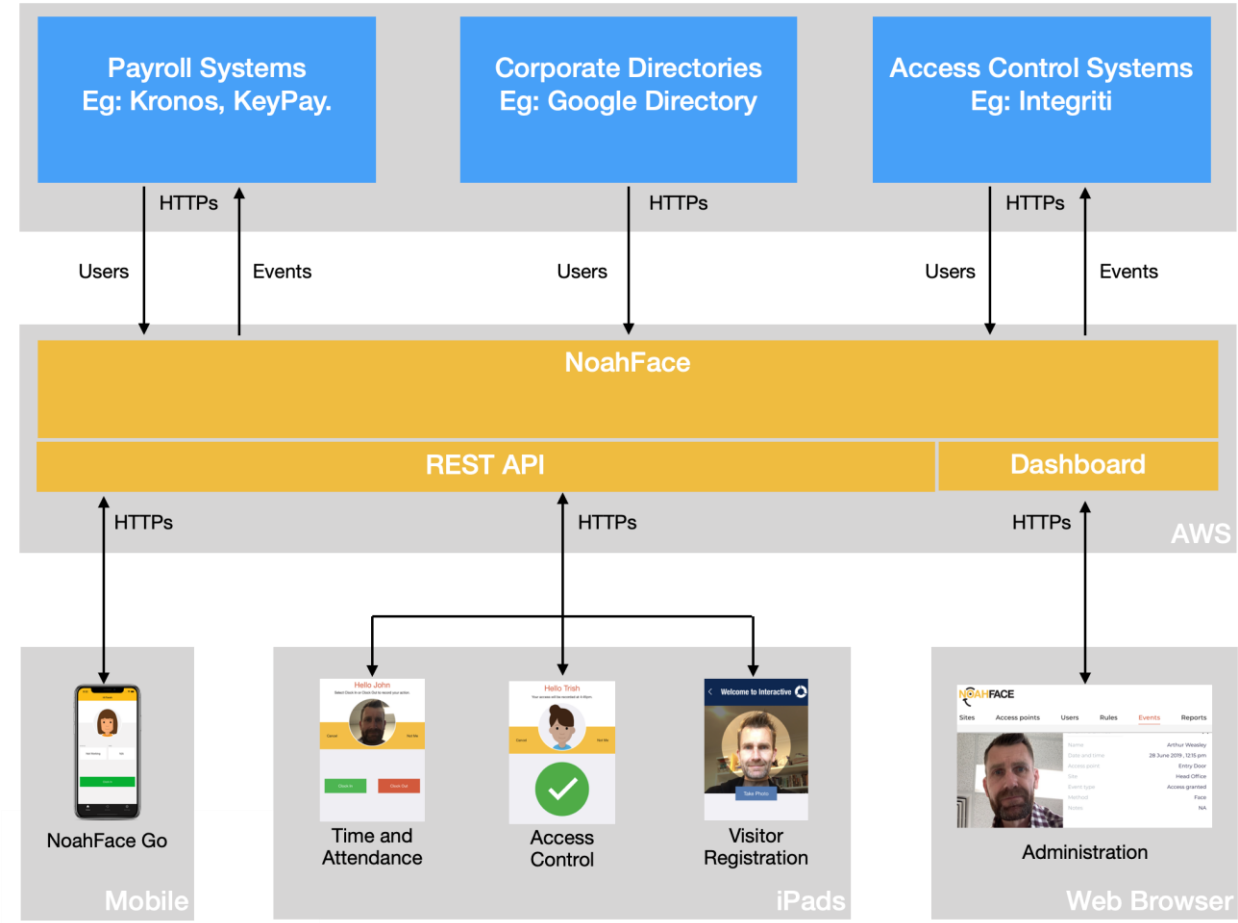
If after reading this document you have further questions about data storage or privacy, we'd be pleased to answer them. Please email us as follows:

Technical Questions: support@noahface.com

Privacy Questions: privacy@noahface.com

Architecture Overview

An overview of the NoahFace architecture can be seen in the diagram below:



Note that:

- The NoahFace platform is hosted in the Cloud on Amazon Web Services (AWS). Structured data is stored in RDS and unstructured data is stored in S3.
- There are a number of clients that connect to the NoahFace platform:
    - The NoahFace Go mobile App, which runs on iOS and Android.
    - The NoahFace App, which runs on iPadOS.
    - The Administration Dashboard, which runs in a Web browser.
- Users are managed in 3rd party systems (ie: Payroll Systems, Access Control Systems, or Corporate Directories) and are automatically replicated to the NoahFace platform and the NoahFace Apps.
- Events are captured by the NoahFace Apps and are automatically replicated to the NoahFace platform and 3rd party systems (ie: Payroll System or Access Control Systems).
- The 3rd party systems may be hosted either in the Cloud or on premise.

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. NB: Non-credit card payment options are also available.
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, an identifying number (eg: an employee number, a member number, etc) 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. For mobile generated events, geolocation is also captured (with consent). If you are screening for elevated temperatures, a measured temperature is also captured.

Video

NoahFace processes video but does NOT store that video under any circumstances.

Photos

When a user registers to use NoahFace, they can choose a profile picture, which can be either a photo (taken at the time of registration) or an avatar (ie: a cartoon). The purpose of the profile picture is to allow users to identify themselves. Users can change their profile picture at any time.

When a user performs an event (eg: clocks in/out or enters a door), an event photo is captured. This event photo is clipped so that only the person's face is captured and that people in the background are not also inadvertently captured. You can configure NoahFace to capture more of the background if you choose to.

* It is possible to configure NoahFace so that event photos are only captured for users who explicitly consent to it. See the section "User Consent" for more information.

Data 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
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. NB: Non-credit card payment options are also available.

Local Storage

Local data 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 data 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 data 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.

Biometric Storage Options

Each time a user registers or uses NoahFace, event photos are captured and biometrics are extracted from these photos. Biometrics are encrypted before they are stored, and are managed by the NoahFace App.

NoahFace provides you with two data storage options for biometrics as follows:

1. Local
2. Cloud

Regardless of how you choose to store your biometrics, NoahFace does not offer any facilities to export biometrics.

Local Biometric Storage

Local biometric storage means that biometrics never leave the iPad on which they are captured. This option is usually used for implementations that have a single iPad.

Cloud Biometric Storage

Cloud biometric storage means that biometrics captured during registration are sent to the Cloud, and from there they are shared to other iPads (there is no direct communication between iPads). This allows users to register at one iPad and then be automatically recognised at other iPads without registering again.

This option is usually used for implementations that have multiple iPads.

Encryption

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

1. The NoahFace Cloud server uses AES-256 encryption to encrypt data at rest.
2. All network traffic between the NoahFace App and the NoahFace Cloud server is encrypted using industry standard TLS/SSL. The SSL certificate used employs 2048 bit keys.
3. Sensitive user identifiable information that is needed locally on the iPads (ie: passcodes and biometrics) is encrypted at rest and stored using Apple's keychain facilities. They Apple KeyChain uses AES-256 encryption. This is important because it means if an iPad is ever stolen, this data cannot be extracted. You can read more about Apple Keychain facilities here:

   https://developer.apple.com/documentation/security/keychain_services

4. Passcodes are hashed (one-way) with SHA-256 before they are stored in the Apple keychain, so even if the Apple keychain was compromised, there is a second level of protection which is generally considered unbreakable on its own.
5. All network traffic between NoahFace and 3rd party systems is also encrypted using industry standard TLS/SSL. For example, if you choose to synchronise your list of users with a 3rd party system (eg: Google Directory, and Access Control System, or a Payroll System), communication with these systems is over TLS/SSL.

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 or a 3rd party backup service. 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 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*.

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.

The NoahFace platform automatically replicates stored data across multiple data centres (see "High Availability" for more information), and takes snapshot backups on a daily basis.

* See the section "Biometric Storage Options" for more information on biometrics storage. If you are using Local biometric storage and you connected a new iPad to replace a broken or stolen iPad, users you would need to re-register.

High Availability

NoahFace recognises that employee focused systems are mission critical to the operation of a business, and has built in high availability at several levels.

Platform

The NoahFace Cloud service runs in Amazone Web Services (AWS) and utilizes multiple AWS availability zones ("multi-AZ") to replicate data across multiple physical data centres and provide high availability in the event of a complete outage of a data centre.

3rd Party Systems

NoahFace sends event data to 3rd party systems from the NoahFace Cloud service. If a 3rd party system is temporarily unavailable, NoahFace will periodically attempt to re-send the data until the 3rd party system is available.

NoahFace App

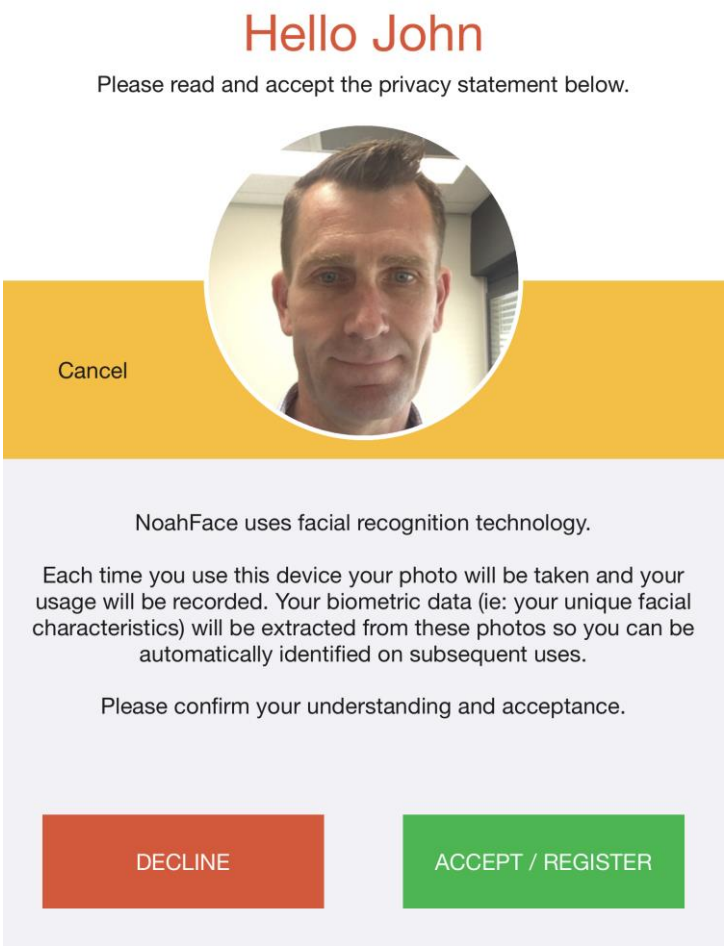
The NoahFace App is designed to continuously operate regardless of network availability.

Facial recognition is performed locally on the device, providing lightning-fast performance at all times.

Events are initially captured and stored locally, allowing users to complete their interaction. Event data is written to the Cloud asynchronously in the background, whenever the network is available.

User Consent

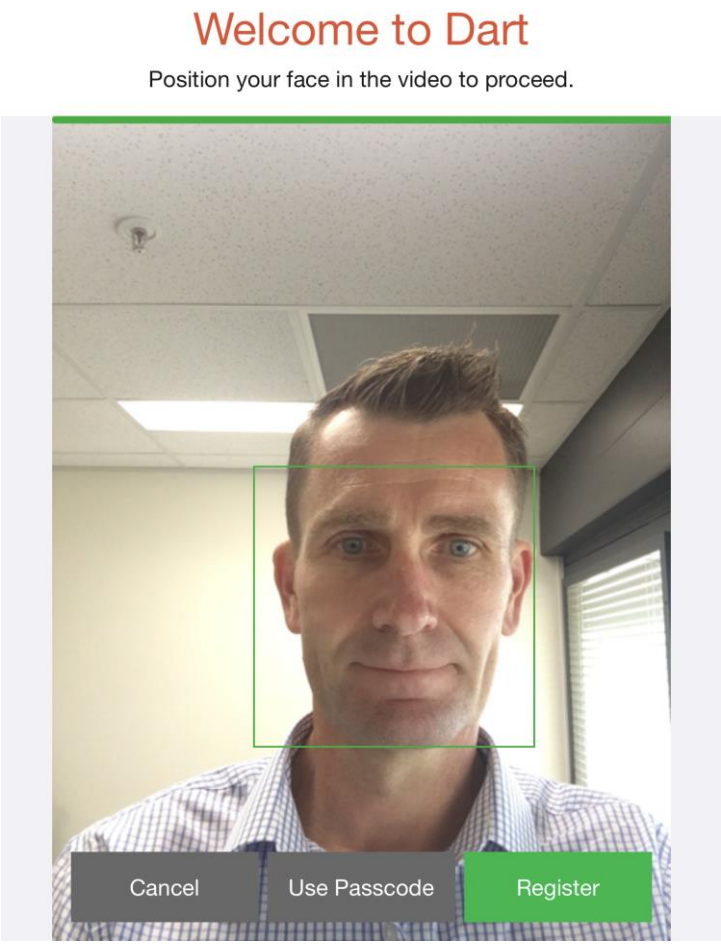
In order to register to use NoahFace, users must consent to their photos being taken and stored and their biometrics being extracted from these photos and stored. Users will see a screen such as the following during registration:



If a user starts the registration process and then declines to provide consent, their photograph is discarded, and biometrics are not extracted.

Manual Use

If you choose to allow it, NoahFace can be configured so that users can record events without using facial recognition. If you do this, an extra button (eg: “Use Passcode”) will appear on the Welcome screen:



There are three possible configuration options:

A. Manual usage is not allowed. Users must register (and consent to the use of facial recognition) in order to use NoahFace to record events.
B. Manual usage is allowed, but a photograph will still be taken. Users must present themselves in front of the camera before the “Use Passcode” button will become active.
C. Manual usage is allowed and no photographs will be taken. Users do not ave to present themselves in front of the camera – the “Use Passcode” button is always active.

Revision History

Revision	Date	Description
1.0	7th Aug 2018	Initial revision.
2.0	3rd Mar 2019	Added section on “Biometric Storage Options” Added section on “User Consent”.
2.1	21st Oct 2019	Added sections on “Video” and “Photo” storage. Expanded “User Consent” section.
6.2	5th Mar 2020	Re-wrote section on “User Consent”. Added section on “Manual Use”.
8.12	30th Oct 2020	Added section on “Architecture Overview”. Added section on “High Availability”. Expanded section on “Backups”. Expanded section on “Encryption”.