SONY

# Privacy and security of the Nimway solution

Privacy is an increasingly sensitive topic as people are coming to realise how little of it they actually have. For this reason, the privacy standards of the Nimway solution go above and beyond industry regulations. In fact, our privacy standards go above and beyond industry regulations.

nimway

# How we protect user privacy

When developing the privacy scheme for the Nimway service, we gathered and incorporated feedback from our users, and made sure to meet all their requirements. In addition, the Nimway team has been involved in worker council and employee meetings with our clients. Feel free to get in touch if you would like us to support you in discussions of this kind.

## Features summary

- Nimway is a voluntary service.
- Employers cannot force employees to use the service.
- Personal information from the Nimway system is not shared with the employer (it cannot therefore be used to monitor employees).
- Sensor data (from meeting rooms and individual desks that are available for everyone) is anonymized. Facility Managers can only see that a space is or has been occupied, not by whom.
- An employee's location information is only uploaded to Nimway when searching for a colleague, or when the person being searched for has accepted.
- Location data is only stored for 60 seconds.
- The find-a-colleague feature is designed to ensure employee privacy. The employee decides whether to share his/her current location or not and the feature is disabled by default.
- Employees can decide whether or not they want to share their location automatically, or just to share it when someone is looking for them.
- Location information from sensitive areas, such as restrooms, is not shared.
- Employees can only search for colleagues who are in the office.
- Employees are always notified when searched for.
- Employees can see earlier searches in a search log.

# Data security

The Sony development process ensures that Nimway undergoes continuous data security reviews and has automated source code analysis to ensure no security degrades are introduced in the production environment.

The Nimway service includes several security controls for personal data:

- HTTPS with HTTP Strict Transport Security (HSTS) enabled from web clients.
- Encryption of all personal data in transfer and at rest.
- Penetration test covering servers, applications and local hardware, conducted by Sony IT Security.
- Continuous endpoint vulnerability scanning by Sony IT Security
- .Amazon Web Services accounts authenticated using multifactor authentication.
- Audit logging is enabled for Amazon Web Services.

Users are authenticated by their corporate email address. All users belonging to a certain email domain, i.e. can only access data within that domain (for instance, building data or other user locations). As such, the Nimway mobile apps are not limited to corporate owned devices - any device can be used as long as the user can be authenticated.

## Personal data
Nimway collects and stores personal data. For the following data Sony acts as controller

## **Location** (optional feature)
The Nimway applications support estimating the location indoor locally in the device. The location information is used to provide wayfinding locally in the device and can also be shared with colleagues if the employee wants.

A number of functions are in place to protect the user's privacy:

1. Employee decides if he/she wants to share their current location automatically or not. This is disabled by default.
2. Locations in sensitive areas, such as restrooms, are not shared.
3. Employees are only allowed to search for others when they're in the office.
4. Employees are notified when searched for
5. Employees can see earlier searches in a search log.

## Email address, name, profile photo
The user's email address, name, and profile photo (optional) are collected from mobile devices through the Nimway application. This data is used to represent the user in the Nimway service.

## Device ID
Device ID is collected in most API calls. This data is used to be able to separate data when a user has multiple mobile devices.

## **Office access** (optional feature)
If the Office access feature is enabled the dates of which a user has office access bookings are stored. Users can choose if colleagues should be able to see their upcoming bookings or not. It is disabled by de-fault.

## **Parking reservation** (optional feature)
If the parking reservation is enabled, the dates of which a user has parking reservations are stored.

## Calendar appointments
Room and user calendar appointment data is collected remotely from the company calendar server. Nimway stores the users' upcoming calendar appointment start and end times, meeting title and location, to be able to show wayfinding on the digital floorplan, but also notify the mobile device of an updated calendar so it can manage its time-to-go notifications.

The customer can control which data is collected and visualised in the Nimway using the room booking solution (for instance, Exchange) and limiting access to Nimway.

## Facility data
Nimway collects and stores building data. Static information is collected initially and is modified in the Nimway management tool e.g. building maps and meeting room details. Dynamic information is continuously and automatically updated e.g. live room occupancy status from occupancy sensors and room booking information from the Nimway room booking solution.

## Data storage and retention

Storage time for personal data

- Calendar data is stored for 24 hours by default.
- The user's positions are saved for 60 seconds, unless otherwise agreed with the customer
- The user's email, name and profile photo are saved as long as the user has a user account

Nimway cloud is hosted on AWS (Amazon Web Services), under a Sony contract. The personal data is stored on S3, DynamoDB and Postgres. Personal Identifiable Information (PII) is always encrypted at rest. Sony also uses AWS S3 checksums and encryption to ensure integrity for stored data and use encrypted transfers.

Sony is the controller of most personal information collected by Nimway unless otherwise specified in the contract with customer. Sony has a controller to processor agreement with Amazon because we use their servers to store information. Calendar data is cached for the maximum number of days in advance a room or desk booking can be made. Default is 1 day.

The optional features, Office access and Parking reservation, store bookings for up to 30 days.

## Data deletion

It is possible to have the entire account deleted when signing out from the Nimway application. The AWS S3 mechanism ensures secure deletion from physical media. All backups of personal data will also have the same retention limits and be deleted automatically on a schedule.

## Data access

Nimway users within a company domain can search for colleagues within the same domain, thus accessing name, email address, profile photos and location of users. Location sharing can be enabled or disabled by each user, based on his or her personal preferences.

Facility managers can see building utilisation data generated from the room booking system and sensors, but they cannot identify individual users.

The optional features Office access and Parking offers an optional secure API where the email address of users that have valid reservations can be accessed for integration with entrance access and monitoring systems.

The usage of this data is regulated through the amendment for the features.

A limited group of people in the Nimway development team has access to Nimway personal data, since they need it to develop and maintain the service.

## Approved by high-profile customers

The Nimway service has been thoroughly reviewed and thereafter approved by high-profile fortune 500 companies in the Banking and Pharmaceutical industries.

## ISO27001 certified business

The Space Solutions Division within SNCE is certified for ISO27001 for the Information Security Management System.

# Sony’s approach to security and privacy

The Nimway service is based on a philosophy of “security and privacy by design”. In other words, Sony’s developers always prioritise security and privacy issues when designing new features of the system. This approach is an established pattern for creating high quality and secure IT systems.

If you have any questions, please feel free to get in touch.

nimway

To find out more about Nimway, contact contact@nimway.com

Or go to our website nimway.com