White Paper

nymi™

Nymi's Alignment with the General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA)

Version 1.0
Jan 2021

Contents

Introduction

At Nymi, we believe that privacy and security of personal data is a human right. Our goal is to simplify the connection of employees to the digital space in a way that is safe, secure, and convenient for the end user. The Nymi Connected Worker Platform (CWP) connects workers from the factory floor to the C-Suite, resulting in a human network that we deliver with private, secure, and user-centric controls. This approach creates organization-wide benefits.

Our solution is comprised of a highly secure wearable component (the Nymi Band™) and an easily deployed enterprise software platform (Nymi CWP) that is suited to any industry. The Nymi Band allows touchless and fully encrypted wireless communication between users and digital systems. On-device biometrics ensure the identity of the user, while integrated sensors convey information about the individual and their environment.

User privacy is a fundamental design requirement for the solutions that we develop and deploy. This document describes our security and privacy practices, and how they align with the General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA).

Checklists

GDPR: Lawful basis and transparency

☑ **Provide clear information about your data processing and legal justification in your privacy policy.**

You need to tell people that you are collecting their data and why (Article 12). You must explain how the data is processed, who has access to it, and how you are keeping it safe. This information needs to be included in your privacy policy and provided to data subjects at the time you collect their data. It must be presented "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

CCPA: Right to know

☑ **The right to know about the personal information a business collects about them and how it is used and shared**

At Nymi, we ensure that there is visibility and transparency about what, how, and why any personally identifiable information (PII) is processed or stored. The Nymi Connected Worker Platform is deployed in some of the most highly regulated environments and in strict compliance with the GDPR. We provide full transparency to our customers and enable them to do the same for their employees. Some resources we provide include:

- Technical white papers and documentation that describe Nymi's security and privacy practices and controls – starting from our manufacturing process to user onboarding best practices.
- Privacy Awareness Training for users, as well as educational handouts and videos, typically provided during user onboarding.
- A privacy statement on our website and privacy policy documentation.
- A companion mobile application, called Nymi Lynk, to provide additional privacy information to users.
- A secure enterprise solution that is built with Privacy by Design principles.

GDPR: Data Security

☑ **Take data protection into account at all times, from the moment you begin developing a product to each time you process data.**

You must follow the principles of "data protection by design and by default," including implementing "appropriate technical and organizational measures" to protect data. In other words, data protection is something you now have to consider whenever you do anything with other people's personal data. You also need to make sure that any processing of personal data adheres to the data protection principles outlined in Article 5. Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need. The point is that it needs to be something you and your employees are always aware of.

CCPA: Right to delete

☑ **The right to delete personal information collected from them (with some exceptions)**

Privacy by Design is a specific methodology and a foundational principle for how we develop and deploys our products and services. Nymi prioritizes user privacy by minimizing the storage of PII. The result is powerful technology that empowers the end user while also protecting their right to privacy and control over their personal information.

In this section, we will describe the different components and features of the Nymi CWP that work together to provide superior security and privacy for user and enterprise:

Nymi Band™

- **Privacy by Design:** First, and foremost, the user's biometric data never leaves the Nymi Band. During enrollment, the user's fingerprint is analyzed by the Nymi Band to create a fingerprint template. The fingerprint template is a mathematical algorithm that is derived from a unique set of features from the fingerprint. During authentication, the fingerprint of the user is matched against the fingerprint

template stored on the Nymi Band. The fingerprint template never leaves the microcontroller unit (MCU) of the Nymi Band and is kept in secure storage, as described in the next bullet point. More information about how biometric data is handled by the Nymi Band can be found in the following section.

- **Memory protection:** The JTAG debug interface is permanently disabled in the MCU to prevent data and code access. There is no USB port on the Nymi Band for data transfer purposes. Therefore, data access and firmware upgrades are feasible only through encrypted Nymi protocols over BLE. Additional read-only regions and a memory firewall protect the bootloader and root-of-trust cryptographic keys and certificates from unauthorized modifications.
- **Secure boot and secure upgrade:** The Nymi Band bootloader verifies the firmware signature during a firmware upgrade and the Nymi Band boot-up, which ensures that only authorized firmware can execute on the Nymi Band.
- **Secure storage:** Sensitive data, including cryptographic keys, root certificates, and the fingerprint template are stored securely on the MCU flash and protected by the memory protection feature described previously.

Nymi Enterprise Server (NES)

NES handles centralized functionalities that are required for the deployment, operation, and management of the Nymi Band and other Nymi software components.

The main functions that NES performs are:

- Allowing storage and retrieval of information that is necessary for the use and management of Nymi Bands: for example, Nymi Band to Nymi user mapping, and dissemination of the NES group policy, through the NES Directory and Policy Service.
- Issuing authentication tokens to Nymi-enabled Applications (NEAs) through the NES Enrollment Service and the Nymi Token Service (NTS).
  *Nymi-enabled Applications are applications that are integrated with the Nymi Band directly using the Nymi SDK.
- Allowing user authentication to Active Directory during Nymi Band enrollment.
- Supporting Nymi Band management and NES group policy configuration through the NES Administrator Console.

Nymi Band Application (NBA)

The Nymi Band Application (NBA) is a Windows desktop application that allows users to enroll their Nymi Band. From an architecture perspective, NBA is a Nymi-enabled Application with special management privileges.

NBA performs the following functions:

- Orchestrates user authentication, Nymi Band authentication, enrollment of a fingerprint template and other authentication credentials.
- Provides the necessary information to NES, which NES stores in a SQL database, to support subsequent management and operation of Nymi Bands.

  NOTE: For more information on storage, please refer to Nymi's ***Storage and Transmission of Personal Data*** document.

Nymi SDK

The Nymi SDK serves two purposes:

- Provides access to the Nymi API (via a C language interface or a WebSocket interface), which enables developers to create NEAs.
- Provides the Nymi Runtime, which includes the Nymi Agent and Nymi Bluetooth Endpoint (NBE) services, that communicates with Nymi Bands via the Nymi Security Protocol.

Nymi SDK contains three components: Nymi Agent, NBE, and Nymi API (NAPI) DLL:

- Nymi Agent facilitates communication between NEAs and the Nymi Bands and maintains knowledge of Nymi Band presence and authentication states. In addition, it provides access to the Nymi API via the WebSocket interface.
- NBE provides local BLE communications with Nymi Bands through the Nymi-provided BlueGiga dongle. NBE also detects Near Field Communication (NFC) taps and reads the NFC Unique Identifier (UID) from detected Nymi Bands.
- NAPI DLL gives NEAs access to Nymi Band functionalities via the Nymi API C interface. It also manages NEA certificates and allows secure communications with Nymi Bands via the Nymi Security Protocol.

GDPR: Data Security

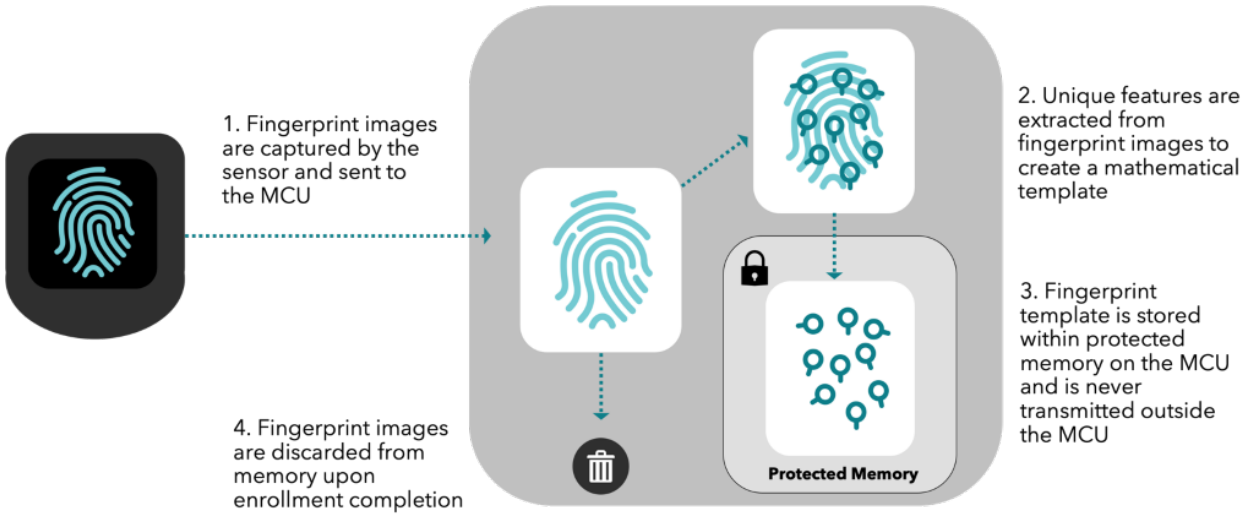
☑ Encrypt, pseudonymize, or anonymize personal data wherever possible.

Most of the productivity tools used by businesses are now available with end-to-end encryption built in, including email, messaging, notes, and cloud storage. The GDPR requires organizations to use encryption or pseudonymization whenever feasible.

The Nymi Band enables handsfree and touchless access to corporate buildings, apps/systems, and services; it also works throughout the day to keep Nymi users safer by protecting their health, safety, and privacy while at work. This requires a method for securely authenticating the user, as well as securely integrating them to various enterprise applications and systems within your company. The following section describes our various technical security controls.

Biometrics on the Nymi Band

The Nymi Band authenticates a user's identity using their fingerprint. During the user enrollment process the Nymi Band's fingerprint sensor analyzes the user's fingerprint to generate a mathematical template based on unique features of the fingerprint. The initial image is discarded, and the mathematical fingerprint template is stored within protected memory (see diagram below). The fingerprint template never leaves the Nymi Band.



The Nymi Band uses ECG (electrocardiogram) sensors for two purposes: 1) to detect liveness by measuring a user's ECG signal against a generic human ECG template that is stored on the Nymi Band, and 2) to ensure that there is a closed electrical loop from the user's wrist to the fingertip of their opposite hand, indicating that the user is indeed wearing the Nymi Band while authenticating with their fingerprint. However, the Nymi Band does not store a fingerprint image, nor does it collect or store any data about the user's unique ECG signal. In other words, the Nymi Band cannot uniquely identify you by your ECG signal, and never transmits any fingerprint or ECG data.

Cryptographic Algorithms and Security Protocols

We leverage cryptographic algorithms in many areas of our solution to provide the following security functions:

- Authentication (of Nymi Bands and NEAs)
- Data encryption (in communication protocols and storage)
- Message authentication code
- Code signing in firmware

Public Key Infrastructure (PKI)

PKI certificates are used for mutual authentication between Nymi Bands and NEAs. The use of certificates enhances security by eliminating the need for key sharing for supporting multiple-terminal operations (large number of NEAs being able to authenticate to a Nymi Band) and permits offline operations of NEAs.

Certificate Enrollment

Nymi Band certificate enrollment is performed during manufacturing:

- The Nymi Band generates a Nymi Band key pair and stores it in the on-band secure storage, and then generates a PKCS #10 Certificate Signing Request (CSR) that is signed by the Nymi Band private key.
- The CSR is then retrieved from the Nymi Band and sent to the Nymi Band Subordinate CA. The CA verifies the CSR, signs the certificate, and returns it to the Nymi Band for secure storage. The Nymi Band private key never leaves the Nymi Band.

  NEA certificate enrollment is performed during first-time execution of the NEA.

- Key generation and CSR creation are performed in a fashion similar to the Nymi Band certificate enrollment.
- NES Enrollment Service and NTS performs additional authentication of the CSR origination point by using AD credentials, verification of CSR subject, and authorization of the CSR using a challenge password.

Nymi Security Protocol

- The Nymi Security Protocol is modeled after TLS 1.2 and provides security for BLE communications with Nymi Bands.
- The first phase of setting up a BLE secure session is called "Validation," and it is akin to a TLS handshake.
    - Validation involves the NEA and Nymi Band performing mutual authentication by using the NEA certificate and Nymi Band certificate and establishing a session key using Elliptic Curve Diffie Hellman (ECDH) with ephemeral keys to achieve perfect forward secrecy.
- After the successful completion of the Validation phase, secure data transfers can happen between the Nymi Band and the NEA.
    - The use of AES-GCM ensures security by providing message encryption, message origin authentication, tamper detection, and (with the inclusion of a message sequence number) replay protection.

For more information about the security of the Nymi Band and the Nymi Connected Worker Platform, please refer to the ***Nymi Security White Paper.***

GDPR: Data Security

☑ Create an internal security policy for your team members and build awareness about data protection.

Even if your technical security is strong, operational security can still be a weak link. Create a security policy that ensures your team members are knowledgeable about data security. It should include guidance about email security, passwords, two-factor authentication, device encryption, and VPNs. Employees who have access to personal data and non-technical employees should receive extra training in the requirements of the GDPR.

At Nymi, we work with companies to ensure that there is visibility and transparency about what, how, and why any PII is processed or stored. The Nymi Connected Worker Platform is deployed in some of the most highly regulated environments in countries around the world, and within strict compliance of the GDPR.

Available resources include:

- Technical whitepapers and documented methodologies on our security and privacy practices starting from our manufacturing process through to onboarding users.
- Training users and making them aware prior to and during the onboarding process with security and privacy post cards and awareness training sessions.
- A privacy statement on our website and privacy policy documentation.

GDPR: Privacy Rights

☑ It's easy for your customers to request and receive all the information you have about them.

People have the right to see what personal data you have about them and how you're using it. They also have a right to know how long you plan to store their information and the reason for keeping it that length of time. You have to send them the first copy of this information for free but can charge a reasonable fee for subsequent copies. Make sure you can verify the identity of the person requesting the data. You must be able to comply with such requests within a month.

Our Customer Success team works with each of our customers to develop an internal communications and deployment plan that ensures Nymi users are properly informed about what personal data must be collected in order to use the solution, including the specific purpose for collecting the data, and how long it will be kept. We also provide best practices on how to provide users with the ability to opt in. In addition, we provide an optional companion mobile app called "Nymi Lynk," which is available on the Apple and Android app stores. Nymi Lynk provides answers to user FAQs and will provide more visibility to the user about what features of the Nymi Band are active according to the policies set by the company and provide links to other Nymi privacy information.

GDPR: Privacy Rights

☑ **It's easy for your customers to request to have their personal data deleted.**

People generally have the right to ask you to delete all the personal data you have about them, and you are required to honor their request within about a month. There are five grounds on which you can deny the request, such as the exercise of freedom of speech or compliance with a legal obligation. You must also try to verify the identity of the person making the request.

Nymi Band users can wipe all of their biometric information and personal data by following a simple operation on their Nymi Band at any time. Also, our Customer Success team works with each of our customers to provide best practices around user onboarding, offboarding and user data deletion processes, which are performed by Administrators at your company, that can be easily integrated into internal workflows.

GDPR: Privacy Rights

☑ **It's easy for your customers to ask you to stop processing their data.**

Your data subjects can request to restrict or stop processing of their data if certain grounds apply, mainly if there's some dispute about the lawfulness of the processing or the accuracy of the data. You are required to honor their request within about a month. While processing is restricted, you are still allowed to keep storing their data. You must notify the data subject before you begin processing their data again.

Nymi users have the ability to stop the Nymi Band from processing data at any time by simply removing the Nymi Band from their wrist, at which point the Nymi Band will deactivate immediately. To reactivate the services on the Nymi Band, the user needs to reauthenticate using their fingerprint while wearing their Nymi Band. Again, the user can perform the *Delete User Data* process on their Nymi Band to erase the fingerprint template and User ID stored on the Nymi Band and reset the device to factory defaults at any time.

Additional Reference Materials

For more information on Nymi Security & Privacy, please refer to the following documents, which can be provided on request:

- ***Compliances and Cybersecurity Framework*** – Oct 2020
- ***Storage and Transmission of Personal Data*** – Dec 2020
- ***Security & Privacy Presentation*** – Dec 2020
- ***Nymi Security White Paper*** – Jan 2021

Please reach out to one of our subject matter experts at info@nymi.com

About Nymi

Nymi has created a world where people and digital systems converge in a manner that is safe, secure, and simple.

We empower workers and help businesses achieve true digital transformation.