Application Privacy Policy – myHCN

1. Purpose of the Application

The myHCN application allows existing subscribers of the company to view information related to their account, including:

• service details
• packages and subscriptions
• invoices and billing information
• support-related information

The application functions exclusively as a viewing tool for data that already exists in the company's internal systems.

The application:

• does not allow account creation
• does not allow users to enter or modify personal data
• does not collect new personal data from users

2. Data Collection

The application does not collect new personal data.

The following are not used:

• usage analytics tools
• user tracking mechanisms
• advertising identifiers
• user profiling for commercial purposes

All information displayed in the application originates exclusively from the company's internal systems for the purpose of providing services to existing subscribers.

3. Maps and Navigation

The application includes a map feature to display company stores or service locations.

Important:

• The application does not request or use the user's location.
• The application does not access GPS or device location data.

When the user selects the "Directions" option, the application opens the device's preinstalled navigation application, such as:

• Google Maps
• Apple Maps

Navigation is handled entirely by those applications and is subject to their own privacy policies.

The application does not receive, store, or process any location data.

4. Notifications and Updates

The application does not use push notification services for advertising or user tracking.

User updates:

• are displayed within the application
• are provided by the company server when the user logs in
The application does not use:
• advertising notifications
• behavioral tracking

5. Use of Firebase
The application uses Firebase services only for displaying dynamic content inside the application.
Specifically:
• Firebase Analytics is not used
• No advertising identifiers are collected
• No user tracking is performed
Firebase is used solely as a tool for delivering dynamic text and image content within the application without collecting user data.

6. Login Security
Access to the application requires secure authentication.
Security measures include:
• encrypted communication via HTTPS / TLS
• authentication tokens with limited lifetime
• temporary account lock after repeated failed login attempts
User passwords are never stored within the application.

7. Data Security
To protect user data, the following technologies are used:
Android
• Jetpack Security EncryptedSharedPreferences
• AES-256 encryption
• key management via Android Keystore
iOS
• token storage in the iOS Keychain
• access policy: WhenUnlockedThisDeviceOnly
Additionally:
• HTTPS communication (TLS 1.2 or higher)
• clear-text traffic disabled
• secure network configurations

8. Data Sharing
The application does not sell, share, or transfer user data to third parties for commercial purposes.
All data processing takes place exclusively within the company's internal systems for the purpose of providing services to subscribers.

9. Data Retention
The application does not store personal data beyond what is strictly necessary

for maintaining the user session.
Upon logout:
• authentication tokens are removed
• session data is cleared
• temporary data is deleted

10. User Rights
In accordance with the GDPR, users have the right to:
• access their personal data
• request corrections
• request restriction of processing
• request deletion where applicable
Requests can be submitted through the company's official customer support channels.

11. Legal Compliance
The application complies with:
• GDPR (EU Regulation 2016/679)
• Greek and European data protection legislation
• Apple App Store and Google Play Store requirements