**VendAPP Privacy Policy**

Last updated: 25.02.2026 | version: 1.0

## I. Introduction

The VendAPP application is committed to respecting the privacy and security of its users' personal data. This document describes the rules for data processing in connection with the use of the VendAPP mobile application, including in particular the use of background location (GPS), NFC, and the camera. Before installing and starting to use the application, please read this Privacy Policy to ensure transparency and understanding of the data processing rules.

## II. Data Controller

As a rule, the controller of the personal data processed via the VendAPP application is the entity on whose behalf you use the application (e.g., your employer or vending operator) that has granted you access to VendAPP ("Organization"). The Organization determines the purposes and means of processing data as part of the process of performing service and operational tasks.

The creator and provider of the VendAPP application is System66 sp. z o.o., with its registered office at ul. Filtrowa 27, 85-237 Bydgoszcz, NIP: 9671457493, REGON: 52389146 (hereinafter: the "Provider"). Privacy contact: biuro@system66.pl
In a typical B2B model, the Provider acts as a data processor on behalf of the Organization under a data processing agreement. If, in your deployment, the roles are regulated differently (e.g., the Provider as the controller within a specific scope), the arrangements of the Organization apply.

## III. Information Collected

For the proper operation and to provide the application's operational features, VendAPP may process the following categories of data:

1. Identification and work-related data: first and last name, phone number, user identifier, Organization identifier, and information about roles/permissions – to the extent necessary for authentication and use of the application.
2. Operational data: information about routes, visits, tasks, completion statuses, confirmations (e.g., code scans), location and device/terminal identifiers, execution reports, and other data entered as part of performing work duties. Data entered or generated in VendAPP is transmitted to the VendSYSTEM (backend) in order to provide operational services and is made available to the Organization within its administrative permissions. The Provider does not sell personal data and does not share it for advertising purposes.
3. Geolocation (GPS) data: when you grant permission to access location, the application may also collect location data in the background (i.e., when the application is not actively open) in order to support route functionality, document the course of visit execution, and ensure operational accountability. The scope may include approximate and/or precise location—depending on the device configuration and the permissions granted. You can change location permission at any time in your device operating system settings; restricting this permission may result in route and visit confirmation features being unavailable.
4. NFC data: VendAPP may use NFC to start/identify a visit, link activities to a specific device or location, and prevent abuse. In this scope, NFC usage events may be processed and—if used in a given deployment—tag/device identifiers.
5. Camera data: VendAPP may use the camera to scan codes (e.g., QR/Barcode) and—if enabled in a given deployment—to take photos documenting the device condition or completion of a service activity. The application does not access the photo gallery without user action.
6. Technical and diagnostic data: device type, operating system version, application version, technical identifiers (e.g., installation identifier), IP address, event and error logs – for security, diagnostics, and maintaining service quality.

## IV. Use of Information

The collected data may be used, in particular, to:

1. Provide and maintain VendAPP services and functionalities (execution of routes, visits and tasks, data synchronization, reporting).
2. Ensure accountability and operational compliance (including confirmation of completed visits and activities, deviation analysis, activity audits).
3. Ensure security (including detecting abuse and protecting against unauthorized access).
4. Provide technical support and develop the application (error analysis, improving stability).

For the purposes described above, VendAPP may process location data also in the background (in accordance with the device permission settings). This data is not used for advertising purposes or marketing profiling.

If additional analytics or reporting tools are used in a given deployment, the Organization or the Provider will inform you about this in a supplement to this Policy or in the deployment documentation.

## V. User Rights

To the extent resulting from personal data protection regulations (in particular the GDPR), you have the right to access your data, rectify it, erase it, restrict processing, data portability, and to object. Where processing is based on consent, you also have the right to withdraw your consent at any time.

Due to the B2B model, requests related to the exercise of your rights should first be addressed to the Organization, which is the data controller. The Provider supports the Organization in fulfilling these rights to the extent resulting from the data processing agreement.

## VI. User Obligations

The user undertakes to:

1. Not attempt to breach the security of the application or the services (including backend services).

2. Not modify or interfere with the application code, bypass security mechanisms, or circumvent access control mechanisms.
3. Use the application in accordance with the permissions granted by the Organization and with operational procedures.

## VII. Notifications

With consent or to the extent permitted by the device settings, users may receive push notifications regarding, among others, task reminders, route changes, operational messages, and service alerts. Notification settings can be changed in the application settings or in the device operating system settings. Disabling notifications may limit timely task execution and the availability of certain functionalities.

## VIII. Security, Data Recipients, and Transfers to Third Countries

VendAPP applies appropriate technical and organizational measures to protect data against unauthorized access, loss, or disclosure. In particular, the following may be used: transmission encryption (TLS/SSL), access control mechanisms, authentication, security event logging, and permission restrictions. Data recipients may include only:

1. The Organization – to the extent necessary to carry out service and operational processes,
2. The Provider and its subcontractors (processors) – solely to the extent necessary to maintain and provide the services (e.g., hosting, infrastructure maintenance, technical support).

As a rule, data is processed within the European Economic Area (EEA). If, as part of providing the services, data is transferred outside the EEA, this will take place only on the basis of appropriate legal mechanisms and safeguards required by law (e.g., standard contractual clauses).

## IX. Changes to the Privacy Policy

We reserve the right to update this Privacy Policy, in particular in the event of legal changes, changes to the application's functionality, or organizational changes. Users may

be informed about material changes via the application, by the Organization, or by e-mail—depending on the adopted communication model.

## X. Data Retention

Personal data is stored for the period necessary to achieve the purposes described in this Policy, in particular for the duration of the Organization's cooperation with the Provider and for the period required by law or justified by settlement and security needs. Detailed retention periods may result from the Organization's policies and the deployment agreement.

## XI. Children's Privacy

VendAPP is a tool intended for business use and is not directed to persons under 18 years of age. We do not knowingly collect children's data. If it is determined that a child's data has been processed, the Organization and/or the Provider will take steps to promptly delete such data or restrict its processing.

## XII. Privacy Contact

For matters related to privacy and personal data protection, first contact the Organizer/Controller (the Organization) that granted you access to VendAPP. You may also contact the Provider at the following e-mail address: biuro@system66.pl.

## XIII. User Account Deletion

In the B2B model, the user account is linked to the Organization. Access to the VendAPP application is granted and revoked centrally from the VendPORTAL system, which is used, among other things, to manage user accounts and their permissions within the Organization. This means that the end user (e.g., a technician/service worker) generally does not delete their account independently directly in the VendAPP application. The Organization using the solution (e.g., an employer/operator) is fully responsible for creating the account, granting permissions, changing them, and deactivating/removing access. Any requests regarding account deletion, access deactivation, restriction of permissions, or the exercise of data-related rights (including data erasure) should be

addressed by the user to the appropriate representative of the Organization in accordance with the procedures in force within that Organization.

After the account is deactivated in VendPORTAL, the user loses the ability to log in to VendAPP and use the application's features. Operational data and activity history (e.g., routes, visits, reports) may remain in the VendSYSTEM system to the extent necessary to ensure continuity of the Organization's processes, accountability of service activities, archiving obligations, and in accordance with the deployment agreement and applicable law. Where the Organization instructs the Provider to delete data to the extent possible and required, the Provider will carry out such instruction in accordance with its role as a processor and the agreed procedures.