

Meridian

Security and Data Protection Statement

Document ID	IM.MERIDIAN.INT.06
Document version	1.0
Date of issue	2026-10-06
Applies to	Meridian 1.1.10.0
Language	English
Publisher	iMobile

Contents

- 1. Deployment model 3
- 2. Data processed 3
 - 2.1. Personal data 3
 - 2.2. Where data is stored 4
 - 2.3. Data sent to the vendor 4
- 3. Access control 4
- 4. Cryptography 4
- 5. Logging and audit 5
- 6. Data export and deletion 5
- 7. Updates and vulnerability handling 5
- 8. Certifications and assessments 6
- 9. Accessibility 6
- 10. Known limitations 6

About this document

This statement describes how Meridian version 1.1.10.0 handles data and which security mechanisms it implements. It describes the product as shipped. It is not a certification and does not replace the customer's own risk assessment.

1. Deployment model

Client and server components, all installed on the customer's equipment.

A client–server system on the customer's own equipment. The program `Meridian.exe` is installed on every workstation from a Windows Installer package and connects over the network directly to a database on the customer's PostgreSQL server; the database is deployed by a script from the database kit. An HTTP API service for external applications can be used in addition: its executable is included in the package as `tools\MeridianDbTool.exe`, while the scripts that install the service are not part of the download set. Vendor servers do not process customer data; the program contacts the iMobile account server `accounts.new-imobile.com` only to activate and check the licence.

When installed on the customer's equipment, the product runs on infrastructure the customer controls, and the vendor has no access to the content processed there. Connections the product makes to third-party services that the customer configures are described in the Product Description.

Independently of the deployment option, the vendor receives the data listed under "Data sent to the vendor".

2. Data processed

2.1. Personal data

- Employees (users): surname, first name, patronymic, date of birth, sex, position, department, work e-mail, phone numbers, Skype name, room number, photograph, login, password hash, date of last sign-in
- Contact persons of counterparties: surname, first name, patronymic, sex, date of birth, position, department, phone numbers, fax, e-mail address
- Counterparties, including individuals and sole traders: name, tax and registration identifiers, addresses, bank accounts
- Customer loyalty cards: card number, phone number, name, date of birth, purchase turnover, bonus balance
- Customers' vehicles: make, model, VIN, registration number, year of manufacture, mileage
- Messages and attachments of the mailboxes connected to the program, and the credentials of those mailboxes
- Attached files and the text of documents, tasks and comments entered by users
- When the HTTP API service is used: login, network address and device name for sign-in attempts, session details
- When the region-specific transport module is enabled: drivers' names, tax number, phone number and driving-licence details, and details of signers
- The e-mail address the program was activated with — in the licence file on the workstation

2.2. Where data is stored

Business data is stored in a PostgreSQL database on the customer's server. Attached files are stored in a place chosen by the customer: a network folder or, by a setting, an S3-compatible store or a WebDAV server. A workstation holds: the encrypted connection file `DBConnect.db` in the program folder, the licence file `%ProgramData%\Imobile\Meridian\license.dat`, logs in `%APPDATA%\Imobile\Meridian\Log`, the attachment cache and downloaded updates in `%LOCALAPPDATA%\Imobile\Meridian`, and parameters in the registry keys `Software\Imobile\Meridian`. The vendor's account server holds the account (e-mail address), licence details and the registration and activation events.

2.3. Data sent to the vendor

- Activation and licence check (`accounts.new-imobile.com`, HTTPS): e-mail address, confirmation code, product identifier, licence key, token, machine fingerprint (a SHA-256 hash); at activation, on the Refresh licence button and at start-up when the stored licence is older than 14 days
- Update check (`new-imobile.com`, HTTPS): a request for the file `latest.json` that carries no customer data, by default no more than once a day; the package is downloaded on the user's command
- Customer business data (goods, documents, customers, employees) is not sent to the vendor

3. Access control

A user signs in with an employee login and password; the program checks the password against the hash in the database. There is no multi-factor sign-in, no single sign-on and no link to directories (Active Directory, LDAP); the desktop program has no lock-out after failed attempts. Rights are set in two layers: the employee's section profile (which sections are visible and what is allowed in them: add, edit, copy, delete, export, report) and roles, which open, make read-only or hide individual buttons, fields and grid columns on the screens. A role is given to an employee personally or to a department, in which case it also applies to subordinate departments; there are 13 standard roles. Changed rights apply from the next sign-in. Access control is enforced by the program: every workstation connects to the database under one PostgreSQL service role with the fixed name `imobile` and a password that is built into the program and is the same for all installations.

4. Cryptography

- User passwords are stored in the database as PBKDF2-HMAC-SHA256 hashes (100,000 iterations, a random 16-byte salt for each password)
- Licence: an ECDSA P-256 signature over a SHA-256 hash is verified with a built-in public key through Windows CNG; the licence file is protected with Windows DPAPI and bound to the computer
- Requests to the vendor's account server and site go over HTTPS provided by Windows (WinHTTP, SChannel)
- The integrity of a downloaded update package is checked against the size and SHA-256 from `latest.json`
- The connection file `DBConnect.db` is an SQLite database encrypted with AES-256 by Devart UniDAC; the key is built into the program
- Mailbox passwords are stored in the database encrypted with RC6 (the DCPcrypt library) with a key built into the program
- Receiving mail over IMAP is protected by TLS provided by the OpenSSL 1.0.2u library
- The connection between the program and the PostgreSQL server is not encrypted by the program (SSL mode is off); data in the database is not encrypted by the program

- The HTTP API service issues session tokens and does not provide TLS itself: the channel is encrypted by the customer's reverse proxy
- The region-specific document-exchange module, hidden in the international configuration, creates detached CAdES-BES signatures through Windows CryptoAPI with a cryptographic provider installed by the customer; no such provider is included in the delivery; exchange credentials are protected with Windows DPAPI
- Requests to an S3-compatible attachment store are signed with AWS Signature Version 4 (HMAC-SHA256); the access keys of the store are kept in the settings in clear text

5. Logging and audit

There is no single log of user actions. Database records keep the author and time of creation, of the last change and of the deletion mark. Changes to tasks (state, assignee, due date, priority and other fields) are written by a database trigger to the task log. The employee record in the database keeps the date of the last sign-in and the program version; failed sign-in attempts in the desktop program are not logged. The HTTP API service keeps sign-in attempts with the address, reason and device for 90 days. Every workstation writes a text log of errors, warnings and activation events to %APPDATA%\Imobile\Meridian\Log. Runs of the mail handler script are recorded in the database.

6. Data export and deletion

Grids on the screens export to Excel; export also works in view-only mode. The database is an ordinary PostgreSQL database owned by the customer: a full export is made with `pg_dump`, a selective one with SQL queries or through the HTTP API. Deleting a record in the program as a rule sets a deletion mark on it and does not erase it physically; final erasure of records and of the whole database is done by the database administrator with PostgreSQL tools. Uninstalling the program does not touch the database; the licence file, logs, attachment cache and registry parameters on the workstation are removed by hand. There is no self-service way to delete the account on the vendor's server: the customer contacts the vendor for that.

7. Updates and vulnerability handling

When a user signs in, the program requests the file

`https://new-imobile.com/download/meridian/latest.json` from the vendor's site (by default no more than once a day) and compares the version in it with its own. A newer version is shown in the About window; the package is downloaded with the Update button, verified by size and SHA-256 and installed only on the user's command by starting `msiexec`. The check can be turned off or pointed at another address with the settings `UPDATE_CHECK` and `UPDATE_URL`. The structure of an existing database is upgraded separately with the script `upgrade-db.ps1` from the database kit of the same version.

Suspected vulnerabilities can be reported through:

- contact form: <https://new-imobile.com/contact>
- e-mail: admin@new-imobile.com

Reports are handled as described in the document "Software Lifecycle, Maintenance and Support".

8. Certifications and assessments

No third-party security certification or audit (for example Common Criteria, FIPS 140-3, ISO/IEC 27001 or SOC 2) is claimed for the product or for the vendor in this document.

9. Accessibility

The accessibility of the interface has not been evaluated and no conformance report against accessibility standards has been prepared. The interface is built from Windows controls and third-party grids; the cashier window is designed to be operated from the keyboard alone. Operation with screen readers, in high-contrast mode and at enlarged scale has not been tested.

10. Known limitations

- The program is not a fiscal cash register: it issues no fiscal receipts, does not control fiscal printers or payment terminals and sends nothing to tax authorities; the cashier window records the sale and the payment kind in the books and prints a non-fiscal slip
- The receipt is printed by an editable Python script on a Windows printer; the supplied script needs a separately installed Python 3 with the pywin32 package, and without it the sale is posted but nothing is printed
- Every workstation connects to the database under one PostgreSQL service role, `imobile`; its name and password are built into the program, are the same for all installations and cannot be changed, so access to the database server has to be restricted by network means
- The connection between the program and PostgreSQL is not encrypted; over untrusted networks a protected channel such as a VPN is required
- The program works without access to the vendor's account server for no more than 14 days from the issue of the licence; it cannot run for long in networks with no internet access
- There is no built-in backup: the database and the attachment store are backed up by the administrator with PostgreSQL and operating-system tools
- No ready-made print templates for documents are supplied: documents can be printed after the administrator loads FastReport templates
- The Documents section shows the list of documents; creating and editing a document card is not available in this version; the deals, claims, correspondence, business-trip and tender sections are not available in this version
- The telephony section is switched off in the navigation: calls from the program are not available in this version
- Receiving mail over POP3 does not store the received messages: IMAP is used for receiving; TLS for IMAP is provided by the OpenSSL 1.0.2 branch, which the OpenSSL project no longer maintains
- Looking up goods by barcode in an external catalogue, loading the vehicle catalogue and reference prices need an external catalogue service that is not part of the delivery; without it only the data entered into the database is used
- A mobile application and the scripts that install the HTTP API service are not part of the download set; the service does not provide TLS itself
- The left navigation does not scroll: with a window lower than about 1130 pixels the bottom sections fall off the edge of the window and cannot be reached with the mouse
- The purchase-price columns of the goods grid in a sale document are hidden by the program unconditionally and cannot be opened by a role; task reminders are generated when the Tasks section is

opened, there is no background scheduler

- The pages of the installation package and the messages of the database scripts are in Russian only; some preset values (the retail customer name, the cash-desk wallets, the sample receipt) are supplied in Russian
- The region-specific document-exchange module is hidden in the international configuration and is outside the scope of this edition of the documentation
- The client program runs on 64-bit Windows only; there are no versions for other operating systems and no web interface

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	1.1.10.0	First issue