

iMobile

Meridian

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.MERIDIAN.US.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	Meridian 1.1.10.0
Language	English
Publisher	iMobile

Contents

- 1. Purpose and status 3
- 2. Product facts 3
 - 2.1. Personal data the product can process 3
 - 2.2. Where data is stored 4
 - 2.3. Data sent to the vendor 4
- 3. Privacy 4
 - 3.1. Roles 4
 - 3.2. What the product provides 4
 - 3.3. What remains with the customer 5
- 4. Accessibility 5
- 5. Software supply chain 5
- 6. Cryptography and export controls 6
- 7. Records and taxes 6
- 8. Government contracts 6
- 9. Language 7
- 10. Documents usually requested and where to find them 7

About this document

This annex supplements the documentation of Meridian version 1.1.10.0 for customers in the United States. It sets out the facts about the product that matter under the local rules named below and shows which obligations stay with the customer.

The annex is a statement by the vendor about its product. It is not legal advice, not a certificate of conformity and not a substitute for the customer's own assessment.

1. Purpose and status

No certification, authorisation or registration by United States federal or state authorities is claimed for the product or for the vendor in this document.

2. Product facts

Item	Fact
Product and version	Meridian 1.1.10.0
Deployment	Client and server components, all installed on the customer's equipment
Customer content on vendor servers	No
Interface languages	The program interface is in English and Russian; the language follows the Windows language and can be switched from the window's system menu. The pages of the installation package are in Russian. The messages of the database kit scripts are in Russian.

2.1. Personal data the product can process

- 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. Privacy

The United States has no single federal privacy statute for the private sector. Contracts most often refer to the state consumer-privacy laws, above all the California Consumer Privacy Act as amended by the CPRA (Cal. Civ. Code § 1798.100 et seq.), and to sector laws.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the business (the CCPA term; "controller" in other state laws). The vendor has no access to that data and is not a service provider for it.

For the data listed under "Data sent to the vendor", which the vendor receives in order to perform the licence agreement, the vendor is itself a business (the CCPA term; "controller" in other state laws).

3.2. What the product provides

- **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.
- **Logging.** 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.

- **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.
- **Encryption.** See the section on cryptography below.

3.3. What remains with the customer

- the notice at collection and the privacy policy;
- answering consumer requests to know, delete and correct, using the export and deletion functions above;
- deciding whether regulated categories of data may be placed in the product. No assessment of the product against HIPAA, GLBA, FERPA, COPPA or PCI DSS is claimed in this document.

4. Accessibility

Federal agencies, and many state bodies and universities, buy information technology against Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), whose standards incorporate WCAG 2.0 Level AA, and ask the vendor for an Accessibility Conformance Report on the VPAT template.

Status of the product: 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.

No Accessibility Conformance Report (VPAT) is provided for this version.

5. Software supply chain

Federal agencies set their own software-assurance requirements (OMB Memorandum M-26-05). An agency may ask a software producer for a statement on secure development practices aligned with the NIST Secure Software Development Framework (NIST SP 800-218) and for a software bill of materials (SBOM).

- Development and release practices are described in "Software Lifecycle, Maintenance and Support".
- Third-party components and their licences are listed in "Delivery Specification and Third-Party Components". The list is human-readable; no SBOM in SPDX or CycloneDX format is provided for this version.
- No secure-development attestation is provided for this version.

6. Cryptography and export controls

The product uses cryptography as follows:

- 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
- The product has not been validated under FIPS 140-3. Where the list above names cryptographic services of the operating system, their validation status is that of the operating system.
- The product is developed and published outside the United States. No U.S. export classification (ECCN) is claimed for it. A customer that exports or re-exports the product from the United States determines its own obligations under the Export Administration Regulations (15 C.F.R. Parts 730–774).

7. Records and taxes

The United States has no certification regime for cash-register or accounting software. No U.S.-specific tax content (sales-tax rates, tax forms, payroll) is claimed for this version. Keeping records for the periods required by federal and state tax rules is the customer's task; backup is described in the Installation and Administration Guide.

8. Government contracts

- **Rights in software.** The software and its documentation are "commercial computer software" and "commercial computer software documentation" within the meaning of Part 12 of the Federal Acquisition Regulation and DFARS 227.7202. U.S. Government end users acquire them with only the rights set out in the vendor's licence agreement.

- **Country of origin.** A statement for the purposes of the Trade Agreements Act (19 U.S.C. § 2501 et seq.; FAR 52.225-5) depends on the contracting entity and is given in the contract; none is made here.

9. Language

This package is supplied in English. This annex is laid out for US Letter paper; the other documents of the package are laid out for A4.

Interface languages of the product: The program interface is in English and Russian; the language follows the Windows language and can be switched from the window's system menu. The pages of the installation package are in Russian. The messages of the database kit scripts are in Russian.

10. Documents usually requested and where to find them

Usually requested	Where it is
Product description, functional specification	Product Description and Functional Specification
Installation and operating instructions	Installation and Administration Guide
User manual	User Guide
Maintenance and support description	Software Lifecycle, Maintenance and Support. Service levels: contract
List of third-party and open-source components	Delivery Specification and Third-Party Components
Security and data-protection description	Security and Data Protection Statement
Accessibility Conformance Report (VPAT)	Not provided for this version
SBOM (SPDX or CycloneDX), secure-development attestation	Not provided for this version; component list as above
Service-provider terms (CCPA), business associate agreement (HIPAA)	Contract, where applicable
Licence agreement, warranties, prices	Contract

Document history

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