iMobile

Meridian

Country Annex — United Kingdom

Vendor statement of facts relevant to local requirements

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

© 2026 iMobile. https://new-imobile.com

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. Data protection — UK GDPR . . . 4
3.1. Roles . . . 4
3.2. What the product provides . . . 4
3.3. What remains with the customer . . . 5
4. Supplier security . . . 5
5. Accessibility . . . 5
6. Accounting records and tax . . . 5
7. Language . . . 6
8. Documents usually requested and where to find them . . . 6

© 2026 iMobile

About this document

This annex supplements the documentation of Meridian version 1.1.10.0 for customers in the United Kingdom. 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 under United Kingdom schemes (including Cyber Essentials) and no registration with United Kingdom 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. Data protection — UK GDPR

The UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, apply to the personal data the customer processes with the product. The supervisory authority is the Information Commissioner's Office (ICO).

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the controller. The vendor has no access to that data and is not a processor 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 controller.

Details of the vendor's establishment and, where Article 27 UK GDPR applies, of its United Kingdom representative are stated in the contract.

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 lawful basis for processing and privacy information to individuals;
- records of processing and, where required, a data protection impact assessment;
- answering individuals' requests with the export and deletion functions above;
- reporting a personal-data breach to the ICO within 72 hours where the law requires it.

4. Supplier security

Central-government buyers require suppliers to hold Cyber Essentials certification for many contracts, and assess cloud services against the NCSC Cloud Security Principles. The facts needed for a supplier assessment are in the Security and Data Protection Statement. No Cyber Essentials certificate is claimed in this document.

5. Accessibility

Public-sector bodies must meet the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018, which point to WCAG 2.2 Level AA; all buyers are subject to the Equality Act 2010.

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 WCAG conformance report is provided for this version.

6. Accounting records and tax

The product keeps business records. Under Making Tax Digital, VAT-registered businesses keep digital records and file through software recognised by HMRC. The product has not been submitted for HMRC recognition, and no United Kingdom-specific tax functions are claimed for this version.

7. Language

This package is supplied in English. English is the language of contracts and documentation in the United Kingdom; no further language version is needed.

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.

8. 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
Processing contract (Article 28 UK GDPR), transfer agreement	Contract; needed only where the vendor processes customer data
Cyber Essentials certificate	Not claimed
WCAG 2.2 accessibility statement	Not provided for this version
Licence agreement, warranties, prices	Contract

Document history

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