

Formata

Security and Data Protection Statement

Document ID	IM.FORMATA.INT.06
Document version	1.0
Date of issue	2026-10-06
Applies to	Formata 1.6.0
Language	English
Publisher	iMobile

Contents

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

About this document

This statement describes how Formata version 1.6.0 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

Server software installed on the customer's infrastructure.

The program is installed on the customer's Linux server. It consists of the `crm_server` process (HTTP API, form engine, scheduler, Python worker processes), a PostgreSQL database, a static web client that the server delivers to the browser, and the CRM application, which is loaded into the database from SQL files. Users work in a browser. Channel encryption (HTTPS) is provided by the customer's reverse proxy. According to the vendor's website the same product is also offered hosted on iMobile servers; this documentation set describes installation on the customer's server.

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 and under "Artificial intelligence functions" below.

The product does not send data to the vendor.

2. Data processed

2.1. Personal data

- User accounts: login, name, roles, department, password hash, active flag
- Customer contact persons and leads: last name, first name, position, company, email address, phone, notes
- Organisational structure data: positions, assignments, managers, delegations
- Correspondence: messages of connected mailboxes with attachments, messages of the internal messenger
- Details of counterparties in warehouse documents
- Log records: who signed in and when, who opened and saved forms, who changed field values
- Any other information the customer enters in note fields, attachments and its own forms

2.2. Where data is stored

All data is stored in the PostgreSQL database on the customer's server. Attachments are stored in a directory on the server disk (by default `uploads` in the service working directory); mail attachments are stored in the database. The user's browser keeps the access token (until the tab is closed), the queue of unsaved actions made while offline and a cache of the shell files.

2.3. Data sent to the vendor

None.

3. Artificial intelligence functions

Lead scoring. If the administrator has configured a key for an external artificial-intelligence service, a scheduler job sends that service the fields of unscored leads every 15 minutes (title, company, contact person, e-mail address, telephone, source, budget) and stores the returned score in the lead record. If no key is configured, the score is computed on the customer's server by built-in rules and nothing is sent to an external service.

4. Access control

Sign-in with a login and password; the server issues a random token that the browser sends in the `Authorization: Bearer` header. After five failed attempts within 15 minutes sign-in for that login is blocked for 10 minutes (configurable). The password of a domain account can be checked by an external identity provider over OpenID Connect. There is no multi-factor authentication. Access control: user roles, a role-to-forms matrix, permissions on individual form controls and table fields, record visibility by owner and organisational structure, sharing of a single record, roles on named queries. External systems use API keys with scopes and a request-rate limit.

5. Cryptography

- User passwords are stored as bcrypt hashes (pgcrypto extension, cost factor 10). A password written in clear text (initial data, the user card in the CRM application) is replaced by a hash at that user's first successful sign-in
- Integration API keys are stored only as a SHA-256 hash
- Outbound webhooks of the core are signed with HMAC-SHA256 (the `X-Formata-Signature` header)
- Attachments are addressed by the SHA-256 hash of their content (deduplication, ETag header); this is integrity control, not encryption
- The server accepts requests over plain HTTP; TLS is provided by the customer's reverse proxy. Outbound script connections to mail servers (IMAP, SMTP) and to the external AI service use TLS through Python
- The program does not encrypt data at rest: database content, attachments and the passwords of connected mailboxes are stored unencrypted and are protected by operating-system and database means

6. Logging and audit

The `sys_audit` database table: sign-in attempts (successful, failed, locked), opening and saving of forms, script runs and errors, access denials, form publication, report exports. The `sys_record_history` table: the old and new value of every changed field for tables placed under observation (by default warehouse documents, their lines, products, warehouses and counterparties). Separate logs are kept for integration API calls, scheduler job runs, background tasks, slow queries and configuration transfers. Service messages go to the system journal (journald). The program sets no retention period for the action log.

7. Data export and deletion

Export: results of named queries and data components as CSV (by a button in the forms that provide one and by a request to the server), records as JSON through the integration API, a full export with standard PostgreSQL tools (`pg_dump`). Deletion: individual records in forms, through the API or by the administrator's SQL queries; attachments are marked deleted and the file is erased once nothing references it; all data by dropping the database and removing the attachment directory. The program has no ready-made procedure for anonymising or erasing all information about one person.

8. Updates and vulnerability handling

There is no automatic update and no check for new versions. A new version is delivered as a new set of files; the administrator replaces the server and web-client files, rebuilds the executable, re-applies the application SQL files without loading the initial data and restarts the service.

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".

9. 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.

10. Accessibility

No accessibility assessment (WCAG or similar) has been carried out. The interface runs in a browser, scales with browser zoom and supports right-to-left layout for Arabic and Persian; some operations (dragging cards on the board, working in the designer) are designed for a mouse.

11. Known limitations

- There are no binary installation packages, no automatic update and no built-in backup tools
- The server does not accept HTTPS connections; a reverse proxy with TLS is required
- There is no multi-factor authentication; sign-in through an external identity provider is limited to a login-and-password check
- Without an external session store (Redis) access tokens and open forms live in process memory and are lost when the service restarts
- Application scripts run in separate processes under an unprivileged operating-system account and a restricted database role, but with no restriction on network access or memory; the right to edit scripts should be given to trusted administrators only
- The `/healthz` and `/metrics` addresses respond without authentication; the telephony event endpoint accepts requests without a key until a key is set
- Changes made in the designer to the stock CRM forms, queries and scripts are replaced by the vendor's version when the application SQL files are re-applied

- Data at rest is not encrypted; the passwords of connected mailboxes are stored in the database in clear text
- The number of seats covered by the licence is not enforced by the program
- AI scoring of leads, when a key for the external service is configured, sends lead fields including contact details to that service; without a key a built-in rule-based calculation is used

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	1.6.0	First issue