iMobile

Formata Tracker

Security and Data Protection Statement

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

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

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. Access control . . . 4
4. Cryptography . . . 4
5. Logging and audit . . . 4
6. Data export and deletion . . . 4
7. Updates and vulnerability handling . . . 4
8. Certifications and assessments . . . 5
9. Accessibility . . . 5
10. Known limitations . . . 5

© 2026 iMobile

About this document

This statement describes how Formata Tracker version 1.0 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 product is installed on the customer's Linux server. It consists of the Formata platform server process `crm_server` version 1.7 (HTTP API, form execution, Python worker processes), a PostgreSQL database in which the tracker occupies its own schema, the static web client that the server delivers to browsers, and the tracker application loaded into the database as SQL files. Users work in a browser. Channel encryption (HTTPS) is provided by the customer's reverse proxy. The server contacts the vendor's account server to 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

- User accounts: login, name, roles, password hash, active flag
- Employee data: department, position, daily working hours, team and access-group membership, Gitea login (for smart commits)
- Work data: issue reporters and assignees, watchers, logged-time records (who, when, how much, comment), step ticks
- Text entered by users: issue descriptions, comments, wiki pages, attachments; these may contain any information
- Issue change history and wiki page versions with the author and time, notifications
- Platform log records: sign-ins, opening and saving of forms, script errors, access denials
- Data from Gitea events: names of commit and pull-request authors, repository page addresses

2.2. Where data is stored

All data is stored in the PostgreSQL database on the customer's server, in the tracker schema. Attachments are stored in a directory on the server disk (the `CRM_UPLOAD_DIR` parameter). The licence state is kept in a file in the server's service directory. The user's browser keeps the access token (until the tab is closed), the selected language and a cache of the shell files.

2.3. Data sent to the vendor

- Licence check: the installation token, product identifier, machine identifier and version number are sent to the vendor's account server; at activation also the licence owner's e-mail address and the licence key. Issues, wiki pages, attachments and user data are not sent to the vendor

© 2026 iMobile

3. 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. There is no multi-factor authentication. Tracker access control: tracker roles (tracker administrator, project manager), project roles (viewer, reporter, developer, manager) granted to an employee, an access group or a team, private and internal projects, wiki-space roles, dashboard permissions. Permissions are checked by database functions on every read and write, including attachment downloads and query-string execution.

4. Cryptography

- User passwords are stored as bcrypt hashes (pgcrypto extension, cost factor 10)
- The inbound Gitea webhook is verified by its HMAC-SHA256 signature; the webhook secret is stored in the database and is available only to tracker functions and the tracker administrator
- The account server's licence reply is verified by its ECDSA P-256 signature; the connection to the account server uses TLS
- The server accepts requests over plain HTTP; TLS is provided by the customer's reverse proxy
- The program does not encrypt data at rest: database content and attachments are stored unencrypted and are protected by operating-system and database means

5. Logging and audit

The change history of every issue (the `trk_history` table): fields with old and new values, status transitions, labels, sprint, estimates and dates, comments, links, attachments, steps, logged time, with the author and time; the full text for titles, descriptions and comments. Wiki page versions (the `trk_page_versions` table) with the author, time and comment. A log of Gitea events. The platform action log (the `sys_audit` table): sign-in attempts, opening and saving of forms, script runs and errors, access denials. The program sets no retention period.

6. Data export and deletion

Export: the issue list for a query string and logged time as CSV; wiki pages, branches and spaces as HTML, Markdown and Word; a full export with PostgreSQL tools (`pg_dump` of the tracker schema). Deletion: issues, comments, own time records, wiki pages and spaces, templates, dashboards in the forms according to permissions; user accounts are deactivated; all data by dropping the tracker schema and removing the attachment directory. The program has no ready-made procedure for anonymising or erasing all information about one person.

7. 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 platform files and rebuilds the executable if needed, replaces the tracker application directory, re-runs `apply.sh` without demo data and restarts the service.

Suspected vulnerabilities can be reported through:

- contact form: https://new-imobile.com/contact

© 2026 iMobile

- 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

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; the query string and its hints work from the keyboard, some operations (dragging board cards and steps) are designed for a mouse.

10. 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
- Notifications are shown in the interface only and are not sent by e-mail
- There is no built-in import from other trackers
- PDF export is done by printing from the browser; Word export produces a .doc file
- Gitea is the only supported source-control system, and the integration is inbound only
- Team charts count completed work by resolution date: an issue reopened later drops out of the week in which it was completed
- Changes made in the designer to the stock tracker forms and scripts are replaced by the vendor's version when the application is re-applied
- Writing requires a valid licence or the trial period; without contact with the account server for longer than the allowed period the program switches to read-only mode
- Data at rest is not encrypted

Document history

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

© 2026 iMobile