iMobile

Formata Tracker

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.TRACKER.US.A1
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. Purpose and status . . . 3
2. Product facts . . . 3
2.1. Personal data the product can process . . . 3
2.2. Where data is stored . . . 3
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 . . . 4
4. Accessibility . . . 5
5. Software supply chain . . . 5
6. Cryptography and export controls . . . 5
7. Government contracts . . . 6
8. Language . . . 6
9. Documents usually requested and where to find them . . . 6

© 2026 iMobile

About this document

This annex supplements the documentation of Formata Tracker version 1.0 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	Formata Tracker 1.0
Deployment	Server software installed on the customer's infrastructure
Customer content on vendor servers	No
Interface languages	Interface, default dictionaries, program messages and notification texts: English, Russian, German, Spanish, French, Italian, Polish, Portuguese (Brazil), Turkish, Japanese, Korean, Chinese, Arabic and Persian (the last two right-to-left). Data entered by users (issue titles, wiki pages, names) is not translated.

2.1. Personal data the product can process

- 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.

© 2026 iMobile

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

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

3.3. What remains with the customer

- the notice at collection and the privacy policy;

© 2026 iMobile

- 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: 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.

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 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
- 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).

© 2026 iMobile

7. 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.

8. 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: Interface, default dictionaries, program messages and notification texts: English, Russian, German, Spanish, French, Italian, Polish, Portuguese (Brazil), Turkish, Japanese, Korean, Chinese, Arabic and Persian (the last two right-to-left). Data entered by users (issue titles, wiki pages, names) is not translated.

9. 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	1.0	First issue

© 2026 iMobile