iMobile

Formata Tracker

Country Annex — United Kingdom

Vendor statement of facts relevant to local requirements

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

© 2026 iMobile

About this document

This annex supplements the documentation of Formata Tracker version 1.0 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	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. 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.** 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 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;

© 2026 iMobile

- 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: 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 WCAG conformance report is provided for this version.

6. 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: 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.

7. 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

© 2026 iMobile

Document history

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

© 2026 iMobile