

Formata

Country Annex — United Arab Emirates and Saudi Arabia

Vendor statement of facts relevant to local requirements

Document ID	IM.FORMATA.AE-SA.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	Formata 1.6.0
Language	English
Publisher	iMobile

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 3
- 3. Data protection 4
 - 3.1. Roles 4
 - 3.2. What the product provides 4
 - 3.3. What remains with the customer 4
- 4. Cybersecurity requirements 5
- 5. Use of artificial intelligence 5
- 6. Electronic invoicing 5
- 7. Accessibility 5
- 8. Language 5
- 9. Documents usually requested and where to find them 5

About this document

This annex supplements the documentation of Formata version 1.6.0 for customers in the United Arab Emirates and the Kingdom of Saudi Arabia. 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, licence or registration by authorities of the United Arab Emirates or of the Kingdom of Saudi Arabia is claimed for the product or for the vendor in this document.

2. Product facts

Item	Fact
Product and version	Formata 1.6.0
Deployment	Server software installed on the customer's infrastructure
Customer content on vendor servers	No
Interface languages	Shell: English, Russian, German, Spanish, French, Italian, Polish, Portuguese (Brazil), Turkish, Japanese, Korean, Chinese, Arabic and Persian (the last two right-to-left). CRM form labels are kept in a translation dictionary in the same languages; some strings produced by queries and scripts are shown in Russian only.

2.1. Personal data the product can process

- 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. Data protection

The following laws apply to the personal data the customer processes with the product:

- United Arab Emirates — Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data; in the financial free zones, the DIFC Data Protection Law No. 5 of 2020 and the ADGM Data Protection Regulations 2021;
- Kingdom of Saudi Arabia — the Personal Data Protection Law (Royal Decree M/19 of 2021, as amended by Royal Decree M/148 of 2023) and its Implementing Regulation, supervised by the Saudi Data and AI Authority (SDAIA).

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.

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

3.3. What remains with the customer

- the legal basis for processing, including consent where the law requires it, and notices to data subjects;
- answering data-subject requests with the export and deletion functions above;
- breach notification to the competent authority;
- data-residency requirements: for installations on the customer's equipment, the customer chooses where that equipment is located, including in-country hosting where a sector regulator requires it.

4. Cybersecurity requirements

Government bodies and operators of critical infrastructure apply the National Cybersecurity Authority's Essential Cybersecurity Controls in Saudi Arabia and the information-assurance standards of the national authorities in the United Arab Emirates, and pass them on to suppliers. The facts needed for such an assessment are in the Security and Data Protection Statement. No assessment of the product against these controls is claimed.

5. Use of artificial intelligence

The product uses large language models as follows. 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.

Content sent to a model provider abroad that contains personal data is a cross-border transfer under the laws named above. The output of these functions is to be reviewed by a person before it is relied on.

6. Electronic invoicing

The product keeps business records. In Saudi Arabia tax invoices are issued through systems integrated with the ZATCA e-invoicing platform (FATOORA); the United Arab Emirates is introducing mandatory electronic invoicing in phases. No integration with these systems and no local tax functions are claimed for this version.

7. Accessibility

Government buyers in both countries refer to WCAG for digital services.

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; some operations (dragging cards on the board, working in the designer) are designed for a mouse.

No accessibility conformance report is provided for this version.

8. Language

This package is supplied in English. Government contracts, and in Saudi Arabia invoices and consumer-facing documents, are required in Arabic. Arabic-language documentation is not part of this package.

Interface languages of the product: Shell: English, Russian, German, Spanish, French, Italian, Polish, Portuguese (Brazil), Turkish, Japanese, Korean, Chinese, Arabic and Persian (the last two right-to-left). CRM form labels are kept in a translation dictionary in the same languages; some strings produced by queries and scripts are shown in Russian only.

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
Data processing and cross-border transfer terms	Contract; needed only where the vendor processes customer data
Documentation in Arabic	Not part of this package
Licence agreement, warranties, prices	Contract

Document history

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