

Formata

Country Annex — European Union

Vendor statement of facts relevant to local requirements

Document ID	IM.FORMATA.EU.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 — GDPR 4
 - 3.1. Roles 4
 - 3.2. What the product provides (Articles 25 and 32) 4
 - 3.3. What remains with the customer 4
- 4. Product cybersecurity — Cyber Resilience Act 5
- 5. Supply-chain security — NIS2 5
- 6. Accessibility 5
- 7. Switching and data retrieval — Data Act 5
- 8. Artificial intelligence — AI Act 6
- 9. Accounting and invoicing rules 6
- 10. Language 6
- 11. Documents usually requested and where to find them 7

About this document

This annex supplements the documentation of Formata version 1.6.0 for customers in the European Union and the European Economic Area. 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 CE marking, EU declaration of conformity or certificate under a European cybersecurity certification scheme is claimed for the product 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 — GDPR

Regulation (EU) 2016/679 (GDPR) applies to the personal data the customer processes with the product.

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.

Details of the vendor's establishment and, where Article 27 applies, of its representative in the Union are stated in the contract.

3.2. What the product provides (Articles 25 and 32)

- **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 lawful basis for processing (Article 6) and information to data subjects (Articles 13 and 14);
- the record of processing activities (Article 30) and, where required, a data protection impact assessment (Article 35);
- answering data-subject requests (Articles 15 to 22) with the export and deletion functions above;
- notifying a personal-data breach to the supervisory authority within 72 hours (Article 33);
- for installations on the customer's equipment, the choice of where that equipment is located.

4. Product cybersecurity — Cyber Resilience Act

Regulation (EU) 2024/2847 sets cybersecurity requirements for products with digital elements placed on the Union market. Its main obligations (conformity assessment, EU declaration of conformity, CE marking) apply from 11 December 2027; the manufacturer's duty to report actively exploited vulnerabilities and severe incidents applies from 11 September 2026.

- No EU declaration of conformity under the Regulation has been issued for this version.
- Vulnerability reports are accepted through the channels named in the Security and Data Protection Statement.
- The period during which security updates are provided is set in the contract.
- The components the product contains are listed in "Delivery Specification and Third-Party Components".

5. Supply-chain security — NIS2

Customers that are essential or important entities under Directive (EU) 2022/2555 must address the security of their supply chain (Article 21(2)(d)). The Security and Data Protection Statement and the Delivery Specification contain the facts usually collected in a supplier assessment.

6. Accessibility

Public-sector buyers apply the standard EN 301 549, which Directive (EU) 2016/2102 uses for public-sector websites and mobile applications. Directive (EU) 2019/882 (European Accessibility Act) has applied since 28 June 2025 to the consumer products and services it lists.

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 EN 301 549 conformance report is provided for this version.

7. Switching and data retrieval — Data Act

Regulation (EU) 2023/2854 gives customers of data processing services the right to switch provider and to retrieve their data. For the vendor-hosted option the product offers the following: 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.

Notice periods and assistance during switching are set in the contract.

8. Artificial intelligence — AI Act

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.

Regulation (EU) 2024/1689 applies to AI systems placed on the Union market. The models involved are general-purpose AI models supplied by third parties or chosen by the customer.

- Article 50 of the Regulation sets transparency obligations, which apply from 2 August 2026. Article 50(2) requires providers of systems that generate synthetic content to mark the output in a machine-readable format; for systems placed on the market before 2 August 2026 it applies from 2 December 2026. No machine-readable marking of output as AI-generated is claimed for this version.
- No use listed in Annex III of the Regulation (high-risk systems) is among the purposes described in the product documentation.
- Where an AI function evaluates data about natural persons, the customer assesses it under Article 22 GDPR (automated individual decision-making, including profiling).
- Content sent to a model provider outside the European Economic Area that contains personal data is a transfer under Chapter V GDPR.

The output of these functions is to be reviewed by a person before it is relied on.

9. Accounting and invoicing rules

The product keeps business records. Electronic bookkeeping, invoicing and cash registers are regulated nationally in the member states. No functions specific to the following rules, and no certificate under them, are claimed for this version:

- Germany — the GoBD principles for electronic bookkeeping (Federal Ministry of Finance letter of 28 November 2019, as amended); structured electronic invoices to EN 16931 (XRechnung, ZUGFeRD);
- France — the electronic-invoicing reform phased in from 1 September 2026;
- Italy — electronic invoicing through the Sistema di Interscambio (FatturaPA format);
- Spain — the invoicing-software requirements of Real Decreto 1007/2023 (VERI*FACTU);
- Poland — the national e-invoicing system KSeF.

A customer subject to these rules confirms before use whether the product may serve as its system of record. The functions the product does have are described in the Product Description.

10. Language

This package is supplied in English. Member states may require the national language for documentation supplied to consumers or to public bodies (for example France, Law No. 94-665 of 4 August 1994). National-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.

11. 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
Technical and organisational measures (Article 32 GDPR)	Security and Data Protection Statement
Data processing agreement (Article 28 GDPR), standard contractual clauses	Contract; needed only where the vendor processes customer data
EN 301 549 accessibility report	Not provided for this version
EU declaration of conformity (Cyber Resilience Act)	Not issued; not yet required
Public-sector standard terms (for example EVB-IT in Germany, CCAG-TIC in France)	Contract; the documents of this package serve as the product description those terms refer to
Licence agreement, warranties, prices	Contract

Document history

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