

Verso

Country Annex — European Union

Vendor statement of facts relevant to local requirements

Document ID	IM.VERSO.EU.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	Verso 2026-09-25 (4bac47a)
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 4
 - 2.3. Data sent to the vendor 4
- 3. Data protection — GDPR 4
 - 3.1. Roles 4
 - 3.2. What the product provides (Articles 25 and 32) 5
 - 3.3. What remains with the customer 5
- 4. Product cybersecurity — Cyber Resilience Act 5
- 5. Supply-chain security — NIS2 6
- 6. Accessibility 6
- 7. Switching and data retrieval — Data Act 6
- 8. Artificial intelligence — AI Act 6
- 9. Language 7
- 10. Documents usually requested and where to find them 7

About this document

This annex supplements the documentation of Verso version 2026-09-25 (4bac47a) 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	Verso 2026-09-25 (4bac47a)
Deployment	Either installed on the customer's infrastructure or used as a service hosted by the vendor
Customer content on vendor servers	Yes, in the vendor-hosted option
Location of vendor servers	Stated in the contract
Interface languages	User sections are fully translated into English and Russian. Eight more languages (Spanish, Simplified Chinese, Hindi, Arabic, Portuguese, French, German, Japanese) are partly translated, with the remaining labels shown in English. The admin console and the custom template wizard are in English only. The language of a presentation is chosen separately when it is created.

2.1. Personal data the product can process

- Accounts: user name, e-mail address (when the account was created by address), password hash, role, creation date and address confirmation date
- Content entered by the user: prompts, instructions, uploaded documents and images, slide text and speaker notes, conversation with the AI assistant; it may contain personal data at the user's discretion
- Usage accounting: user identifier, provider, model, purpose of the call, token counts and time of every model call; credit ledger history
- Payment details (cloud service): payment identifier at the payment provider, items bought, amount, status; the program does not receive or store payment instrument details
- Technical data: client network addresses in the nginx logs inside the container; a session cookie in the user's browser
- In the on-premises licence file: the customer's e-mail address

2.2. Where data is stored

On-premises: all data stays on the customer's server in the container data directory `/app_data` (on the host, the `app_data` directory next to `docker-compose.yml`): the SQLite database `fastapi.db` or an external PostgreSQL or MySQL database set with `DATABASE_URL`, the settings file `userConfig.json`, images, exported files, fonts and templates, and the presentation memory store `mem0`. Uploaded source documents sit in the container's temporary directory and are removed when the service starts; the text extracted from them is kept in the presentation memory. In operation an on-premises installation does not contact the vendor's servers: the licence is verified locally, there is no update check and no usage analytics is sent; content leaves the customer's server only in calls to external model, image and search providers, if the administrator has connected any. Cloud service: the same data is stored on the vendor's servers, and content is passed to the model providers chosen by the vendor.

2.3. Data sent to the vendor

- When an on-premises licence is ordered: the customer's e-mail address and the chosen edition; both are written into the licence file. In operation an on-premises installation does not contact the vendor's servers
- In the cloud service: the user's account on the vendor site (e-mail address) used for sign-in, credit purchase records and the credit spending history

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.

In the vendor-hosted option the vendor processes customer content on the customer's instructions and acts as a processor; the customer remains the controller.

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.

The processing agreement required by Article 28 GDPR is concluded as part of the contract and is not included in this package. The location of the vendor's servers is given in the facts table. Where personal data is transferred outside the European Economic Area to a country without an adequacy decision, the transfer is based on the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, likewise as part of the contract.

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 user name (or e-mail address) and password; the roles are administrator and user. The first account becomes the primary administrator; other accounts are created by an administrator, and open e-mail registration is off by default. Each user has a separate workspace: presentations, templates, images and conversations are available only to their owner (filtering by owner in database queries and in file paths). Provider settings, user management and API keys are available only to an administrator in a browser session. The API and MCP use access keys issued by an administrator; a key acts on behalf of the administrator who issued it. Failed sign-in attempts are limited: 5 per 5 minutes per client address and name, and 10 requests per minute per address at the nginx level. There is no multi-factor authentication, no directory (LDAP) integration and no SAML or OIDC sign-in; a sign-in link signed with a shared secret (HMAC-SHA256) is available.
- **Logging.** There is no separate audit log of user or administrator actions; sign-ins and account changes are not logged by the application. What is kept: service messages in the container's standard output (including search queries and image descriptions during generation, and paths of processed files), nginx logs inside the container, an append-only credit ledger and a table of token usage for every model call. The program does not limit how long these records are kept.
- **Export and deletion.** A user exports presentations to PPTX and PDF and deletes them in the Dashboard section. Deleting a presentation removes its record, slides and assistant conversation from the database; exported files, images and presentation memory entries are not removed automatically. An administrator deletes a user account together with the presentations, templates and file directories it owns; credit and token accounting records remain with the identifier of the deleted user. There is no single action that exports all data of an account. All data of an on-premises installation is erased by deleting the data directory. In the cloud service only the vendor can delete an account: users cannot delete their own account.
- **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) has been carried out. The interface is a web application; some controls carry text labels for assistive technology; the slide editor draws the slide on a canvas; the editor provides keyboard shortcuts; right-to-left layout is enabled for the Arabic interface language.

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: A user exports presentations to PPTX and PDF and deletes them in the Dashboard section. Deleting a presentation removes its record, slides and assistant conversation from the database; exported files, images and presentation memory entries are not removed automatically. An administrator deletes a user account together with the presentations, templates and file directories it owns; credit and token accounting records remain with the identifier of the deleted user. There is no single action that exports all data of an account. All data of an on-premises installation is erased by deleting the data directory. In the cloud service only the vendor can delete an account: users cannot delete their own account.

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

8. Artificial intelligence — AI Act

The product uses large language models as follows. Language models draft the outline and the slide text, choose slide layouts, revise the outline and slides at the request of the AI assistant, convert the slides of an uploaded PPTX file into template layouts and, where an image-generating provider is connected, create images. The functions run only on a user's action: starting generation, sending a message to the assistant, creating a template or an image. The model receives the prompt and instructions, the text extracted from attached documents, the outline, the content of the slides concerned and, for template creation, images of the slides; an image provider receives image descriptions or stock search queries; a web search provider, when search is switched on, receives search queries. On premises the recipient is the external provider or the local model server set by the customer's administrator; with a local model the content does not leave the customer's network. In the cloud service the providers are chosen by the vendor. No marking that content was created with AI is added to slides or exported files.

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. 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: User sections are fully translated into English and Russian. Eight more languages (Spanish, Simplified Chinese, Hindi, Arabic, Portuguese, French, German, Japanese) are partly translated, with the remaining labels shown in English. The admin console and the custom template wizard are in English only. The language of a presentation is chosen separately when it is created.

10. 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	2026-09-25 (4bac47a)	First issue