

iMobile

Verso

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.VERSO.US.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. Privacy 4
 - 3.1. Roles 4
 - 3.2. What the product provides 5
 - 3.3. What remains with the customer 5
- 4. Accessibility 5
- 5. Software supply chain 6
- 6. Cryptography and export controls 6
- 7. Use of artificial intelligence 7
- 8. Government contracts 7
- 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 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	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. 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.

In the vendor-hosted option the vendor processes customer content on the customer's instructions and acts as a service provider; the customer remains the business (the CCPA term; "controller" in other state laws).

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).

The contract terms that the CCPA requires between a business and its service provider (Cal. Civ. Code § 1798.140(ag)) are part of the contract, not of this package.

3.2. What the product provides

- **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 notice at collection and the privacy policy;
- 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) 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 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:

- Passwords: Argon2 hashing (pwplib and argon2-cffi libraries); bcrypt hashes and the earlier PBKDF2-HMAC-SHA256 format are accepted and rehashed at sign-in
- Session: a JWT signed with HMAC-SHA256 (a 32-byte secret generated at installation) in a cookie with the HttpOnly and SameSite=Lax attributes, lifetime 30 days; the Secure attribute is not set in the shipped container configuration, because the internal proxy passes the HTTP scheme to the application
- Licence: an Ed25519 signature over canonical JSON, with the public key built into the verification module (cryptography library); the installation fingerprint is computed with SHA-256
- Service signatures: HMAC-SHA256 for the sign-in link from the vendor account area, HMAC-SHA512 for payment provider notifications; address confirmation tokens are stored as SHA-256 digests
- Transport: the container serves plain HTTP without TLS; channel protection for users is provided by the customer's reverse proxy, and by the vendor in the cloud service; external model providers are called over HTTPS
- There is no encryption at rest: the database and files are stored in the clear; provider API keys are stored in the database and in the `userConfig.json` file, API access keys and webhook secrets in the database, and the session signing secret in `userConfig.json`, all in clear text
- 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).

7. Use of artificial intelligence

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.

There is no federal statute on artificial intelligence in commercial software. State laws are developing and mainly address automated decisions with significant effects on individuals; whether the customer's use of these functions falls under them depends on that use. The output of these functions is to be reviewed by a person before it is relied on.

8. 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.
- **Cloud authorisation.** No FedRAMP authorisation is claimed for the vendor-hosted option.

9. 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: 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

Usually requested	Where it is
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	2026-09-25 (4bac47a)	First issue