

Verso

Security and Data Protection Statement

Document ID	IM.VERSO.INT.06
Document version	1.0
Date of issue	2026-10-06
Applies to	Verso 2026-09-25 (4bac47a)
Language	English
Publisher	iMobile

Contents

- 1. Deployment model 3
- 2. Data processed 3
 - 2.1. Personal data 3
 - 2.2. Where data is stored 4
 - 2.3. Location of vendor-hosted data 4
 - 2.4. Data sent to the vendor 4
- 3. Artificial intelligence functions 4
- 4. Access control 4
- 5. Cryptography 5
- 6. Logging and audit 5
- 7. Data export and deletion 5
- 8. Updates and vulnerability handling 5
- 9. Certifications and assessments 6
- 10. Accessibility 6
- 11. Known limitations 6

About this document

This statement describes how Verso version 2026-09-25 (4bac47a) handles data and which security mechanisms it implements. It describes the product as shipped. It is not a certification and does not replace the customer's own risk assessment.

1. Deployment model

Either installed on the customer's infrastructure or used as a service hosted by the vendor.

The application runs in a single Docker container: an nginx front proxy (HTTP, container port 80) routes requests to the web interface (Next.js), the API server (FastAPI) and the MCP server. Data is kept in `/app_data`: an SQLite database by default, or an external PostgreSQL or MySQL database set with `DATABASE_URL`. No language model is included in the image: the application calls an external provider with an API key or a local model server (Ollama, LM Studio, any server with an OpenAI-compatible API). An on-premises installation adds the licence verification module. The cloud service is the same application on the vendor's servers, with sign-in through the vendor site account.

When installed on the customer's equipment, the product runs on infrastructure the customer controls, and the vendor has no access to the content processed there. Connections the product makes to third-party services that the customer configures are described in the Product Description and under "Artificial intelligence functions" below.

In the vendor-hosted option the vendor operates the service and processes customer content on its servers on the customer's behalf.

Independently of the deployment option, the vendor receives the data listed under "Data sent to the vendor".

2. Data processed

2.1. Personal data

- 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. Location of vendor-hosted data

Stated in the contract.

2.4. 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. Artificial intelligence functions

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.

4. 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.

5. Cryptography

- 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

6. Logging and audit

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.

7. Data 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.

8. Updates and vulnerability handling

On-premises: the vendor supplies a new image (or source) and package; the administrator rebuilds and restarts the container, and the database schema is upgraded at start-up by Alembic when `MIGRATE_DATABASE_ON_STARTUP=true` is set. The program has no automatic update and no update check. The cloud service is updated by the vendor.

Suspected vulnerabilities can be reported through:

- contact form: <https://new-imobile.com/contact>
- e-mail: admin@new-imobile.com

Reports are handled as described in the document "Software Lifecycle, Maintenance and Support".

9. Certifications and assessments

No third-party security certification or audit (for example Common Criteria, FIPS 140-3, ISO/IEC 27001 or SOC 2) is claimed for the product or for the vendor in this document.

10. Accessibility

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.

11. Known limitations

- Presentation content is written by a language model and may contain inaccuracies; the result depends on the chosen model and must be reviewed by a person
- There is no release numbering of its own; the interface does not show a version number
- One container and one server worker process: generation runs as in-process tasks, a restart interrupts running generations (finished slides are kept); there is no horizontal scaling or high-availability configuration
- The licence technically blocks only the start of presentation generation; the number of users and the edition features in the licence file are not enforced by the program
- No multi-factor authentication, no SAML or OIDC sign-in and no LDAP integration; a user cannot change or recover a password without an administrator, who resets it
- Open registration should not be enabled on an on-premises installation; accounts are created by the administrator
- No audit log of user or administrator actions
- No encryption at rest; provider API keys and access keys are stored in clear text; TLS is not part of the container
- Quantitative limits: up to 50 slides per presentation, up to 8 attachments per prompt, files up to 100 MB, slide images up to 5 MB, and by default no more than 3 simultaneous generations per account
- Fonts are not embedded in an exported PPTX: the look of the text on another computer depends on the fonts installed there
- Deleting a presentation does not delete exported files, images or presentation memory entries; there is no export of all data of an account
- Isolated network: building the image needs internet access; fonts from the theme catalogue are loaded by the browser from Google Fonts; the image contains text recognition data for English only; the vendor has not audited the own network activity of third-party libraries (Mem0 in particular)
- Creating a custom template from a PPTX file is designed for models that can analyse images; the result is not guaranteed with other models
- The admin console and the template wizard are in English only; eight of the ten interface languages are partly translated; the Help link leads to the English documentation of the Presenton project
- In the cloud service the model providers are chosen by the vendor; a cloud user cannot connect an own API key for presentation generation
- Credits in the cloud service interface are topped up through a single payment provider that accepts cryptocurrency, or with a promo code

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	2026-09-25 (4bac47a)	First issue