NODRIVE

Security & Zero-Knowledge Overview

Public description of the Beta security model

Version 1.0 • 23 August 2026 • Beta

Contents

1. What Zero-Knowledge Means in Nodrive

Nodrive is designed to encrypt file content, filenames and directory structure on the user's device before data leaves the device. In the current Beta Fiscalbox does not offer Hosted storage for file content: data stays local or is sent encrypted to storage selected by the user.

2. Key Hierarchy

- User Key (UK): a random 256-bit key from which the material used to protect disks and files is derived.
- Password-derived key: derived locally using Argon2id; it unlocks the User Key and does not directly encrypt files.
- The password-derived key is ephemeral and is not persisted in plaintext.
- In the current Beta, the wrapped User Key is stored on the local device and is not held by the backend as a recovery escrow.

3. Authentication

According to the current technical model, Nodrive uses OPAQUE authentication so that the password is not sent to the server in plaintext. Communications with the backend are protected by TLS. The Nodrive backend is currently hosted on Google Cloud Platform in Europe.

4. Local Storage and "Your Storage"

For local disks, encrypted data resides on the storage selected by the user. With "Your storage", the client sends encrypted blocks to the authorised provider. For Google Drive, Nodrive uses OAuth, does not know the Google password and stores the authorisation token only on the user's PC.

5. What May Still Be Visible

- To the Fiscalbox backend: account existence, email/technical identifiers, authentication and security events, app version and technical data required for the service.
- To the user-selected storage provider: the identity of its own customer, encrypted objects and infrastructure metadata such as number, size and timing.
- To Google Analytics on the website, after consent: website usage, browser/device information, sessions and approximate location under the GA4 configuration.
- To Fiscalbox, only when submitted by the user: optional technical diagnostics for troubleshooting.

6. What the Backend Does Not Store in the Beta

- Users' file content as Nodrive Hosted storage.
- Google passwords or passwords for other connected providers.
- The Google Drive OAuth token, which remains on the user's PC.
- The User Key in plaintext or server-side escrow of the wrapped User Key in the current Beta.

7. Declared Limitations

- A device compromised by malware, keyloggers or elevated privileges may bypass application-level protections.
- A weak password remains a risk if an attacker obtains the encrypted material required for offline guessing.
- External applications and the operating system may create temporary files, autosaves, previews, indexing data or swap outside Nodrive's direct control.
- Loss of both password and recovery key may make data unrecoverable.
- A third-party provider may become unavailable, change its terms or delete objects.
- No security statement should be read as a guarantee of absolute invulnerability.

8. Feature Status

Beta features
The installed build, release notes and current technical documentation are authoritative. Planned features - such as Hosted storage or server-side key portability - must not be treated as active until they are actually deployed and verified.

9. Security Reports

Technical or security reports can be sent to info@nodrive.cloud. Do not send passwords, recovery keys or cryptographic keys in support messages.