

FileShark Data Processing & Roles Addendum

Last Updated: August 9, 2026

This Data Processing & Roles Addendum ("Addendum") clarifies the data protection roles of the parties in connection with the FileShark software, which is offered by Legal Authority Lab, LLC under its Legal and Code brand ("Legal Authority Lab") and purchased and operated by you (the "Customer"). Capitalized terms not defined here have the meanings given in the Terms of Use.

1. You Control the Roles

After purchase, you own your copy of FileShark and control how it is used. Legal Authority Lab, LLC and its Legal and Code brand are not involved in your operation of the software, do not access, host, or process the data you handle with it, and are neither the Controller nor the Processor of that data. You determine those roles.

Because you operate FileShark, you determine the purposes and means of processing any personal data handled through it, including the files, forms, and signatures you collect from your clients ("Customer Data"). You (or a party you designate) are the Controller of Customer Data, and you decide who acts as any Processor. Legal Authority Lab is neither the Controller nor the Processor of Customer Data and is not a party to your processing of it.

2. Legal Authority Lab Does Not Process Customer Data

Because you install and operate the Software and configure its third-party services under your own accounts, Legal Authority Lab does not access, host, receive, or process Customer Data. If you separately request optional support and choose to share specific information with us for that purpose, we will use it only to provide the support you requested and at your direction.

3. Your Service Providers and Sub-processors

Any third-party services you connect to your FileShark deployment — such as payment processing, file storage, email delivery, and malware scanning — are selected and controlled by you and act as your service providers or sub-processors. You are responsible for entering appropriate data processing terms with them and with your clients. Annex 2 lists the categories of services FileShark can integrate with; the specific providers and accounts are yours to choose.

4. Data We Process for the Sale

The limited personal data that Legal Authority Lab processes to sell and support the Software — such as your account and billing information — is handled by Legal Authority Lab as an independent controller under its Privacy Policy, not as your processor.

5. Your Responsibilities

- Determine and, where required, document the Controller and Processor roles for Customer Data.
- Provide required notices to, and obtain any required consents from, your clients.
- Configure and operate the Software's security features appropriately for your risk and obligations.

- Enter data processing agreements with your own vendors and clients where required.
- Comply with all data protection and other laws that apply to your handling of information.

6. Security Capabilities of the Software

FileShark provides the following technical capabilities for you to configure and operate. Legal Authority Lab does not operate them on your behalf:

- Encryption of data in transit using TLS.
- Encryption of stored files at rest using AES-256-GCM, with a unique per-file data key wrapped by a key held in a key-management service (envelope encryption), supporting key rotation.
- Private, nonpublic object storage for uploaded files and related work product.
- Malware scanning of uploaded files before they are stored.
- Role-based access controls scoped to each matter, optional multi-factor authentication, and password hashing.
- Audit logging of key actions, and rate limiting on authentication and upload endpoints.

7. Governing Law; Precedence

This Addendum is governed by the laws of the State of Florida, consistent with the Terms of Use. If there is a conflict between this Addendum and the remainder of the Terms regarding data protection roles, this Addendum controls.

8. Contact

Questions about this Addendum may be directed to support@legalauthoritylab.com or 7900 Nova Drive, Suite 205, Davie, Florida 33324.

Annex 1 — Nature of Data You May Process in FileShark

For your reference when documenting your own roles. You determine and control the following:

Categories of Data Subjects: Your personnel and authorized users; your clients and other individuals you invite to upload documents; and individuals whose information appears within submitted files.

Types of Personal Data: Names, email addresses, organization and role, and account credentials (stored hashed); the contents of uploaded files and form responses; electronic signature records (signer name, IP address, timestamp, and document hash); and usage and log data.

Special categories: May be included within Customer Data at your discretion. You are responsible for the lawfulness of collecting and handling such data.

Annex 2 — Integratable Service Categories (Your Sub-processors)

FileShark can integrate with the following categories of services, which you select and contract with directly under your own accounts:

- Payment processing — for example, Stripe.
- Encrypted object storage — for example, Amazon S3 or an S3-compatible provider such as Cloudflare R2, Google Cloud Storage, or self-hosted MinIO.

- Transactional email delivery — for example, Amazon SES, Resend, or another SMTP provider.
- Malware scanning — for example, self-hosted ClamAV or an equivalent scanning provider.