

# ORINEX WORKSPACE - DATA PRACTICES

For district technology, privacy, and procurement staff  
ORINEX Systems LLC | support@orinexsystems.com

## THE SHORT ANSWER

ORINEX DOES NOT RECEIVE CUSTOMER DATA OR STUDENT DATA DURING ORDINARY OPERATION OF THE CURRENT STANDARD ON-PREMISES CONFIGURATION.

ORINEX Workspace is installed on infrastructure controlled by the district and uses credentials controlled by the district. In the current standard configuration, Google Workspace Customer Data - including information concerning students - is read directly by the district's installation and processed and stored on district-controlled systems. It is not transmitted to, hosted by, or made accessible to ORINEX or its licensing provider.

The Software contacts Keygen LLC for license activation and validation. That transaction includes the application-supplied License Data described below and ordinary network and request metadata associated with the connection. A customer requesting support may also elect to provide diagnostic information to ORINEX.

## INFORMATION YOU PROVIDE DIRECTLY TO ORINEX

ORINEX receives ordinary business and contract information when you request a quote, sign an Order, designate notice contacts, request support, or pay an invoice. That may include names, job titles, business email addresses, telephone numbers, postal addresses, purchase-order information, billing records, and Support Data you choose to provide. This is separate from Customer Data, which is processed locally by the Software on your own systems.

## CURRENT SERVICE PROVIDERS

Keygen LLC - licensing, activation, validation, machine fingerprints, seat state, and signed machine files.

PythonAnywhere - licensing.orinexsystems.com for notices, contacts, provisioning, update metadata and downloads, publishing, and installer delivery; a separate application at admin.orinexsystems.com handles internal quote-to-cash functions and related commercial/customer records.

Postmark - transactional notice delivery and delivery/bounce evidence. Amazon SES is supported in code as an alternative but is not currently used.

Google Workspace/Gmail - ordinary commercial correspondence and Support Data only when a customer voluntarily sends it to ORINEX.

Stripe - payment-processing infrastructure, currently configured with test keys.

Cloudflare Pages - marketing site only, with no licensing role and no Customer Data.

Support bundles are generated locally and reach ORINEX only if the customer administrator chooses to send them. There is no in-app support-bundle upload path and no ORINEX remote-access path. ORINEX will identify the current provider, the function it performs, the data categories involved, and principal processing-location information then reasonably available in this statement or on written request. ORINEX does not represent that a separate formal provider or subprocessor schedule exists unless one has actually been created and published.

## WHAT LEAVES YOUR NETWORK

The Software itself sends three categories. A fourth block below describes what ORINEX's notice service uses and creates when the fallback path is used - that information does not come from your network, but it concerns you and is disclosed here for completeness.

**APPLICATION-SUPPLIED LICENSE DATA** The information the Software deliberately sends for license administration:

|                            |                                                                              |
|----------------------------|------------------------------------------------------------------------------|
| <b>license key</b>         | identifies the license                                                       |
| <b>machine fingerprint</b> | a persistent cryptographic hash derived from hardware and system identifiers |
| <b>hostname</b>            | the name of the machine, e.g. PSD-ARCHIVE                                    |
| <b>platform</b>            | the operating-system family, e.g. "windows"                                  |
| <b>installation ID</b>     | assigned by the licensing service                                            |

**AUTOMATICALLY ASSOCIATED CONNECTION AND REQUEST INFORMATION** Information the network and the licensing provider attach to the transaction regardless of what the application sends. Depending on the provider's configuration and logging practices this may include:

- source IP address
- request date and time
- API path and method
- response status
- user agent
- selected request and response headers
- request and response logs containing the application-supplied License Data

**LICENSING NOTICE EVENT DATA (only when your mail path is unavailable)** The Software normally sends licensing notices through the mail server you configure. If that path is unavailable or delivery fails, it sends a minimal event to an ORINEX-controlled notification service so that the notice can be delivered and evidenced:

- opaque customer or Order identifier
- installation identifier
- event type
- first-detected timestamp
- a fixed sentence written by ORINEX describing the condition
- a fixed sentence written by ORINEX describing how to resolve it
- an ORINEX email address for you to reply to

The agreement also permits, but the software does not currently send: an opaque license identifier, software version, event-schema version, a unique event identifier, a replay-protection value, and delivery status. Section 1.11 of the agreement states the maximum; the list above is what is actually transmitted today.

The application does not intentionally send Customer Data, student information, the raw license key, the machine fingerprint, the hostname, or the configured or licensed Workspace domain through this event. It contains no contact information of yours - the two sentences and the reply address above are ORINEX's own. Business email addresses you supply as notice contacts are held by the notice service to address the notice, as described below, and may reveal an organizational email domain.

## DELIVERY RECEIPTS FOR NOTICES SENT THROUGH YOUR OWN MAIL SERVER

When an operational notice is delivered successfully through your own mail server, the Software transmits to ORINEX a short receipt as described in EULA Section 3.5(k): the notice identifier, a one-way hash of the notice content, the dispatch timestamp, and the receiving mail server response.

It contains no recipient address, no notice text, and none of your data. Its only purpose is so that the evidence of a notice is not held solely on your own server.

No period in the Agreement runs from receipt, and no notice is a condition of the Software continuing to operate during the License Term. The receipt evidences dispatch and the receiving server response; it is not a trigger for suspension or other enforcement.

**NOTICE CONTACTS AND DELIVERY RECORDS** To address and evidence the notice, the service also uses the business contact information supplied in your Order and creates records such as the notice template or content hash, recipient, dispatch time, provider message ID, receiving-server response, bounce, retry, fallback, and receipt evidence. Ordinary network and security metadata is also generated by the service.

The notice function of that service, and the credentials it uses, are limited to delivering and evidencing notice.

To be precise about what the host does rather than what one of its functions does: the same ORINEX-operated service also answers the version-manifest check described under OTHER CONNECTIONS above, and serves the installer itself when an administrator chooses to download an update. Saying it "exists only" for notice would no longer be accurate.

What matters for you is unchanged, and applies to every one of those functions: none of them has any ability or authority to suspend a license, change a domain, alter an entitlement, accelerate or reset a timer, or cause an installation to lock.

None of the categories above is intended to include Google Workspace directory records, student or staff records, files, groups, calendars, device records, audit events, or other Customer Data.

License verification happens at activation and approximately once every 24 hours.

**A NOTE ON IDENTIFIABILITY** These fields generally identify a license or an installation rather than a student. A hostname, network address, or persistent machine identifier may nevertheless identify or be associated with an individual in some configurations - for example, where the Software is installed on a workstation named after the person who uses it. If that matters to your review, install on a server or rename the machine.

## OTHER CONNECTIONS THE SOFTWARE MAKES

### Google APIs

Direct from your server, using YOUR credentials. ORINEX is not in this path.

- Your mail server Alert and report emails you configure, sent to recipients you choose, through your own server.

### Update check

The Software asks an ORINEX-operated service whether a newer version exists. This is a version query only: it sends no information about you, your users, or your Google Workspace, and it never installs anything. You choose whether to download and run an update. It runs about four times a day while the application is running, and when an administrator clicks Check for updates in Settings. Like any web request it reveals your source IP address and the time of the request to that service. Note this is the same service used for the licensing notice fallback described above, but on an unrelated schedule: the update check runs whether or not your mail path is working, and whether or not the notice fallback is configured.

### Update download

If you choose to download an update, the Software asks that same ORINEX service for the installer and proves your license is current in order to get it. THAT REQUEST SENDS YOUR LICENSE KEY. It is sent in a request header rather than in the web address, so it does not appear in browser history or in an address bar. ORINEX configures the service not to record the key in its application logs.

To be precise about the limit of that statement: a request can also pass a reverse proxy, content-delivery network, monitoring agent, or security tooling, each of which may log request headers under its own configuration and practices. ORINEX's statement that the key is not recorded in application logs applies to the application layer; provider-side logging is governed by the relevant provider's configuration and practices.

- This happens only when an administrator clicks to
- download. It does not happen during the routine version
- check above, and it sends nothing about your users or
- your Google Workspace.

## WHAT THE SOFTWARE CAN DO TO YOUR GOOGLE WORKSPACE

The Software is an administrative tool and makes changes using the Google credentials you supply. Capabilities worth naming explicitly for a privacy or procurement review:

**EVALUATION SAFETY.** Evaluation licenses are technically blocked at the central command-execution layer from performing the irreversible operations listed in the Evaluation Order, including domain-wide permanent Gmail deletion, permanent user/group/organizational-unit deletion, permanent Drive-file deletion, mobile-device wipe, and ChromeOS deprovision. Reversible administrative operations remain available, including offboarding that suspends an account and moves it to an organizational unit without deleting the account. User-interface hiding is supplemental; the central execution control is authoritative.

Domain-wide message removal. An administrator can search every mailbox in the domain by Gmail search query and permanently delete matching messages. This exists for phishing response. Deletion bypasses Trash and cannot be undone. A count-only preview runs first and a typed confirmation is required.

Scheduled bulk operations. Bulk actions - suspend, delete, move between organizational units, reset password, force password change, device deprovision - can be scheduled to run at a future time with no operator present. The administrator who scheduled the action is recorded.

Account security actions. Password reset, forced password change at next sign-in, forced sign-out, suspension, and deprovisioning.

Shared drive membership. Adding or removing shared drive members is performed by acting as a drive organizer, because the Google API provides no other route. Restricted to administrators and recorded in the action log.

Approximate login location. Login audit events are labelled with a country derived from the source IP address, so that sign-ins from outside your home country can be flagged. THIS LOOKUP IS ENTIRELY LOCAL - the Software uses a database file installed alongside it and makes no network request of any kind to resolve a location. No address or location leaves your network.

Every one of these is initiated by one of your own administrators, executed with your own credentials, and recorded in the local action log. ORINEX cannot trigger any of them.

## WHAT STAYS ON YOUR SERVER

ORINEX Workspace stores what it reads in local databases on the machine you installed it on:

| DATA                                                                      | WHERE          | HOW LONG                                         |
|---------------------------------------------------------------------------|----------------|--------------------------------------------------|
| Directory, device, group, license, calendar data                          | Local cache    | Refreshed from Google                            |
| Google audit events - admin and login                                     | Local database | 90 days                                          |
| Google audit events - Drive activity                                      | Local database | 30 days                                          |
| ORINEX administrator accounts                                             | Local database | Indefinite                                       |
| Action Log records                                                        | Local database | 1 year default; Indefinite option                |
| Bulk-operation backups and undo records                                   | Local files    | 7 days                                           |
| Scheduled-operation definitions and their run history                     | Local database | Until you delete them                            |
| Alert rules and scheduled-report definitions                              | Local files    | Until you change them                            |
| Operational-notice records and delivery evidence                          | Local database | Indefinite                                       |
| Audit-ingestion statistics                                                | Local file     | Until reset                                      |
| Offline country-lookup database (used for sign-in location)               | Local file     | Shipped with the installer; read-only            |
| ORINEX administrator sign-in secrets: two-factor seeds and recovery codes | Local database | Until the administrator is removed or re-enrolls |
| Configuration (credentials encrypted at rest)                             | Local file     | Until changed                                    |

On the two-factor row specifically, because "credentials encrypted at rest" is too vague to be useful in a security review: each administrator's two-factor seed is encrypted using the Windows data-protection service tied to this machine, and recovery codes are not stored at all - only one-way hashes of them are kept, so a recovery code cannot be read back out of the database even by someone holding the file.

Activity and Action Log controls. Workspace-facing action and undo records are Customer Data stored on the Customer's server. In ORINEX Workspace 3.8.2, the Action Log has a one-year default retention period, a customer-selectable Indefinite option, deletion by date range, delete-all capability, CSV export, and full database/CSV archive export. Exact Gmail search strings are not durably logged; Drive filenames or titles are omitted where an opaque file identifier is sufficient; and free-form Google/API error text is normalized before durable storage. The separate undo log remains available for seven days. The separate Compliance audit dataset follows the retention controls documented for that feature and is not changed by the Action Log setting. Customer controls its server and backups and is responsible for exporting records it needs to retain beyond the configured period.

## IF YOU BUY AN IMPLEMENTATION SESSION

The optional implementation session is a single remote meeting of about ninety minutes. There is no remote-access software involved and nothing is installed to allow ORINEX in later. What ORINEX personnel may see is whatever you choose to show on a screen share you control.

The rules for that session:

- you host the session and control what is shared, and can stop at any time
- ORINEX will never ask for a Google password, an OAuth secret, or an administrator credential, and you should never provide one
- no unattended or persistent access is installed, requested, or available
- you should avoid displaying student or staff records that are not needed to complete the configuration
- anything ORINEX sees during the session is treated as your confidential information
- the session is not recorded unless both parties agree in advance

ORINEX does not retain a copy of anything shown during the session. If a configuration file or log is genuinely needed afterwards, you send it, and it is Support Data under the agreement.

## COMMON PROCUREMENT QUESTIONS

### DO YOU SIGN A DATA PRIVACY AGREEMENT?

- ORINEX will review your district's required privacy or security addendum
- and work in good faith toward mutually acceptable terms appropriate to the
- product's actual data practices. Because the current standard
- configuration is not designed to transmit student data to ORINEX, the
- parties may use an appropriate "no student data received" schedule or a
- tailored addendum.

### ARE YOU A "SCHOOL OFFICIAL" UNDER FERPA?

- In the current standard configuration, the district does not disclose
- education records to ORINEX through ordinary operation of the Software.
- Whether the district nevertheless requires ORINEX to be designated
- contractually as a school official is a matter for the district and the
- parties' applicable agreement.

### DO YOUR STAFF HAVE ACCESS TO OUR SYSTEM?

- The current standard configuration contains no ORINEX-operated
- remote-access feature. If you request support, you choose what diagnostic
- information to send us, and you can review it first. Information you send
- is treated as confidential, is used only for support and related
- troubleshooting and security purposes, is limited to personnel with a need
- to know, is not used for advertising or AI training, and is deleted on
- your request subject to any legal retention requirement.

### WHO ARE YOUR SERVICE PROVIDERS OR SUBPROCESSORS?

Keygen LLC handles licensing, activation, validation, machine fingerprints, seat state, and signed machine files.

PythonAnywhere hosts [licensing.orinexsystems.com](https://licensing.orinexsystems.com) for notices, contacts, provisioning, update metadata and downloads, publishing, and installer delivery. A separate PythonAnywhere application at [admin.orinexsystems.com](https://admin.orinexsystems.com) handles ORINEX's internal quote-to-cash functions and related commercial/customer records.

Postmark provides transactional notice delivery and delivery/bounce evidence. Amazon SES is supported in code as an alternative but is not currently used.

Google Workspace/Gmail is used for ordinary commercial correspondence and receives Support Data only when a customer voluntarily emails it to ORINEX. Stripe is the payment-processing infrastructure and is currently configured with test keys. Cloudflare Pages hosts the marketing site only and has no licensing role or Customer Data.

If you choose to send diagnostic information for support, it may pass through the email, storage, and security providers ORINEX then uses to operate support. ORINEX will identify those providers on request. They are not part of ordinary product operation and receive nothing unless you send it. No provider described above is intended to receive Customer Data or student data during ordinary operation of the current standard configuration.

### WHAT HAPPENS TO OUR DATA IF WE STOP PAYING?

Your data is on your server and stays there. Nonpayment does not by itself cause the Software to disable, degrade, suspend, reduce tier, or shorten the License Term. ORINEX's remedies for nonpayment are the contractual notice, cure, collection, and termination remedies in the Agreement. Ordinary licensed functionality ends only when a valid termination becomes effective or the stated License Term expires, subject to any transition or limited-access rights expressly

provided by the Agreement and the Documentation.

Expiry or effective termination does not delete, encrypt, or alter Customer Data or the Customer's Google Workspace environment. Google Workspace remains manageable through Google's own administrative tools and any other tool the Customer chooses to use.

#### **WHERE IS YOUR DATA HOSTED / WHAT IS YOUR CLOUD SECURITY POSTURE?**

- ORINEX does not host your Customer Data, so there is no hosting posture to
- assess for it. The security questions that matter for this product are
- largely about YOUR server: who can reach it, how it is patched, and how
- the Google credentials on it are protected. We are happy to walk your team
- through hardening it, and to answer questions about how License Data is
- handled.

#### **DO YOU SELL OR SHARE DATA? DO YOU USE IT FOR ADVERTISING OR AI TRAINING?**

- ORINEX does not receive Customer Data or student data during ordinary
- operation and does not sell or use such data for advertising or AI
- training.
- ORINEX and its providers process limited License Data, connection
- metadata, Licensing Notice Event Data, notice contact information, notice
- records, ordinary business records, and Support Data for licensing,
- security, notice, support, legal compliance, billing, and related
- operational purposes. ORINEX does not sell those categories or use them
- for targeted advertising or AI training.

#### **WHY THIS IS DIFFERENT FROM A CLOUD PRODUCT**

Most district software is a hosted service: your data goes to the vendor, and your privacy review has to assess their infrastructure, their staff, their subprocessors, their breach history, and their deletion practices.

ORINEX Workspace inverts that. The software comes to your data. Because district Google Workspace records are not intentionally transmitted to ORINEX's licensing systems, a compromise limited to those licensing systems would not ordinarily expose the district's Google Workspace records, and your existing Google Workspace security and access controls remain the controls that matter most.

This does not eliminate every consideration - software distribution, support transfers you initiate, and any future change in configuration still warrant review - but it substantially narrows the surface your privacy office has to assess.

#### **QUESTIONS**

[support@orinexsystems.com](mailto:support@orinexsystems.com)

We are glad to complete security questionnaires, join a call with your privacy officer, or review your district's addendum.

-----

Document status. Effective date: August 23, 2026. Technical baseline verified against ORINEX Workspace 3.8.2. This Data Practices statement is versioned independently from application build numbers. A later application build that does not materially change a disclosed data flow, data category, provider function, retention rule, customer control, or access practice does not by itself require a new Data Practices effective date. ORINEX will update this statement when a material change affects a disclosure in it. This document is informational and does not amend a signed agreement. Any configuration or support arrangement involving additional data transfers must be documented separately.