

Privacy Policy

Status	Current
Version	1.1
Date	23 July 2026

1 Introduction

Wavelet Systems Ltd (“Wavelet,” “we,” “us,” or “our”) is committed to handling information responsibly and transparently. This Privacy Policy describes how we collect, use, store, and protect information in connection with the infrastructure, hosting, and related services (the “Services”) we provide. It applies to information Wavelet collects and uses as a controller, as described in Section 2. It does not govern information that Wavelet processes on a Client’s behalf, which is addressed separately in that section.

You accept this Privacy Policy at signup, alongside our Terms of Service, or by using the Services. Terms defined in the Terms of Service have the same meaning in this Privacy Policy unless otherwise stated.

2 Our Two Roles

This distinction determines which parts of this policy apply.

Information we control. When you create an account, contact us, or pay us, we decide how and why that information is used. We are the controller of this information, and this policy governs it.

Information you place on our infrastructure. When you run workloads or store content on our Services, that data may include personal information about your own users, employees, or customers. We process it only on your instructions. You are the controller and we are your processor. This policy does not govern that data; your own privacy notice does, and you remain solely responsible for ensuring its collection and use complies with applicable law. If one of your users contacts us about their data, we will refer them to you.

Data processing agreements. Where you are subject to a data protection law that requires a written agreement between controller and processor, Wavelet will enter into a data processing agreement with you covering the processing described in this section. Contact legal@waveletsys.com to request one. Where a data processing agreement is in place, it governs Wavelet’s processing of Hosted Content, and this policy governs only the information for which Wavelet is the controller.

3 Information We Collect

3.1 Client Information

Wavelet collects the following categories of information directly from Clients:

(a) contact information, such as name, email address, and phone number;

- (b) billing information, such as billing address, tax identifiers, and transaction history;
- (c) communications, such as email messages, support requests, and correspondence with your account representative; and
- (d) technical information, such as domain names, service configurations, and project-related technical details.

3.2 Technical and Usage Data

In the course of providing the Services, Wavelet may automatically collect or have access to:

- (a) server and access logs, such as IP addresses, request timestamps, and related traffic information;
- (b) performance data, such as resource usage, uptime metrics, and error logs; and
- (c) security data, such as unauthorized access attempts or anomalous traffic patterns.

3.3 Payment Information

Payments are processed by Stripe, Inc. Wavelet does not receive or store full payment card numbers or security codes. Stripe collects and processes card details directly and, in relation to payment processing, acts as an independent controller for fraud-prevention and regulatory purposes. Where Stripe performs identity verification at Wavelet's request, it acts on Wavelet's instructions in relation to that verification, while remaining an independent controller for its own fraud-prevention and regulatory purposes. Stripe's handling of your information is governed by Stripe's own privacy policy.

3.4 Identity Verification

When Wavelet acts as your Local Internet Registry and allocates internet number resources or submits requests to ARIN on your behalf, applicable policy, regulation, or legislation may require Wavelet to verify your identity before or during provision of the Services. Identity verification is not required for all Clients and is requested only where a specific obligation applies.

Where identity verification is required, you will be asked to submit a government-issued identity document, such as a driver's license, state ID card, or passport, to Stripe, Inc., Wavelet's identity verification partner. Stripe collects, validates, and stores these documents. Wavelet does not download, copy, or store identity documents on its own systems.

Wavelet is able to view a submitted document through Stripe, and will do so only where Stripe flags the document for manual review and Wavelet is required to verify it. Wavelet instructs Stripe to retain identity documents only for as long as they may be required for regulatory purposes, as described in Section 6, and to delete them thereafter.

4 How We Use Information

Wavelet uses collected information for the following purposes:

- (a) providing, operating, maintaining, and improving the Services;
- (b) billing and invoicing;
- (c) client support and communication;
- (d) security, abuse prevention, and network integrity;
- (e) identity verification, where applicable;
- (f) service-level monitoring, where a commitment applies; and

(g) compliance with legal obligations, including sanctions and export-control screening.

Wavelet does not sell, rent, trade, or otherwise monetize Client information or user data, and does not use it for advertising or marketing to third parties.

5 Data Storage and Security

5.1 Storage Location

Client information described in Section 3, including contact, billing, communications, and technical information, is stored on infrastructure located in the United States. Wavelet does not store Client information outside the United States. Backups of this information are held on Wavelet's own infrastructure within the United States.

Hosted Content is stored in the location or locations associated with the Services you have provisioned. Wavelet provides hosting from infrastructure it controls or rents in the United States (New York and Ohio), Canada (Toronto), and Australia (Sydney). Wavelet's London facility is a network point of presence only; Wavelet does not offer hosting or store Hosted Content there.

Operational logs. Wavelet generates operational and audit logs at each point of presence for the Services hosted there. Wavelet does not log the content of network traffic.

Access logs record connection and request metadata, including IP addresses and timestamps. These logs are not generally associable with an identified individual, and Wavelet does not use them to identify individuals except where necessary to investigate abuse, a security incident, or a matter of network integrity.

Audit logs record actions taken in connection with a Client's Services and identify the Client only by an internal account identifier; they do not contain names, contact details, or other directly identifying information. That identifier can be linked to a Client through Wavelet's billing records, which are held in the United States.

Network transit. Wavelet's network includes points of presence in the jurisdictions listed above. In the ordinary operation of the internet, traffic to and from Wavelet's network may transit through any of these points of presence or through third-party networks, and Wavelet does not control the routing of traffic once it leaves its network. Transit routing is not storage; Wavelet does not retain Client information or Hosted Content at a point of presence solely because traffic has transited through it.

5.2 Security Measures

Wavelet implements reasonable and industry-appropriate technical and organizational measures to protect information against unauthorized access, disclosure, alteration, or destruction, including encryption of data in transit, access controls limiting administrative access, contractual restrictions on access by infrastructure providers as described in Section 7.2, active monitoring for unauthorized access and anomalous activity, and regular application of security patches to its infrastructure.

Client information, including billing information, is held on encrypted storage and is not accessible to Wavelet's infrastructure providers.

Hosted Content is not encrypted at rest by default. Where you operate your own servers, encryption of data at rest is your responsibility. For managed hosting, Wavelet can arrange encryption at rest on request; contact Wavelet if your own obligations or risk assessment require it.

5.3 No Absolute Guarantee

No security system is impenetrable, and Wavelet cannot guarantee absolute security against all threats. In the event of a confirmed security breach affecting your personal information, Wavelet will notify you promptly and in accordance with applicable law.

Where Wavelet becomes aware of a confirmed security breach affecting personal information for which a Client is the controller, Wavelet will notify that Client without undue delay and in any event within seventy-two (72) hours of confirming the breach. The notification will describe, to the extent known at the time, the nature of the breach, the categories and approximate volume of data affected, the likely consequences, and the measures Wavelet has taken or proposes to take. Wavelet will provide further information as it becomes available.

6 Data Retention

Wavelet retains information only as long as necessary for the purposes described in this policy or as required by law:

- (a) Account and Client information is retained for the duration of the relationship and for up to twelve (12) months following termination, after which it is securely deleted or anonymized, except where a longer period is required by law or by the following items.
- (b) Billing and tax records are retained as required by applicable tax and accounting law, which may exceed the period in the preceding item.
- (c) Hosted Content is made available for export for the period specified in your Order or Signed Agreement following termination. Where no such period is specified, Hosted Content is made available for export for thirty (30) days following termination. After the applicable period, Wavelet has no obligation to retain Hosted Content and will securely delete it.
- (d) Access and audit logs are retained for the duration of their security and operational use, after which they are deleted or anonymized.
- (e) Identity documents are held by Stripe, not by Wavelet. Wavelet instructs Stripe to retain them for the duration of the service requiring verification and for a further twelve (12) months following termination, after which they are deleted, unless a longer period is required by law.
- (f) Sanctions and export-control screening records are retained for the period required by applicable law or regulation.

7 Disclosure of Information

7.1 No Sale of Information

Wavelet does not sell, rent, or otherwise disclose Client information or user data to third parties for commercial purposes.

7.2 Service Providers and Infrastructure

Wavelet processes payments and, where applicable, identity documents, through Stripe, Inc., which is bound by its own terms and applicable law.

Wavelet rents physical infrastructure and network capacity from third-party facility and connectivity providers. These providers supply hardware, space, power, and connectivity, and do not process Client information or Hosted Content on Wavelet's behalf. Client information is held on encrypted storage and is not accessible to these providers. In relation to all other data held on that infrastructure, Wavelet's agreements with these providers prohibit access without prior notice to Wavelet and Wavelet's written permission, except where they are compelled to do so by law enforcement or valid legal process. All other operations, including email, monitoring, and backups, are performed by Wavelet on infrastructure it controls.

Other than as described above, Wavelet does not share Client information with third-party subprocessors. If this changes, Wavelet will update this policy and, where required, provide notice.

7.3 Legal Disclosure

Wavelet may disclose information where required by applicable law or valid legal process, including subpoenas, court orders, and lawful government or law-enforcement requests, or where Wavelet believes in good faith that disclosure is necessary to protect the rights, property, or safety of Wavelet, its Clients, or the public. Where legally permitted, Wavelet will notify the affected Client before disclosure. In some circumstances Wavelet may be legally prohibited from providing such notice.

7.4 Business Transfers

In the event of a merger, acquisition, or sale of substantially all of Wavelet's assets, Client information may be transferred to the successor entity, subject to this policy continuing to apply. Wavelet will provide reasonable notice to affected Clients before any such transfer.

8 Your Responsibilities as Controller

As the controller for data you collect through your own services, you are solely responsible for:

- (a) publishing and maintaining a compliant privacy notice for your own users;
- (b) obtaining any required consents for your data collection and processing;
- (c) complying with all privacy and data protection laws applicable to your data, including the Children's Online Privacy Protection Act (COPPA) where relevant;
- (d) promptly notifying Wavelet of any known or suspected data breach affecting data hosted on Wavelet's infrastructure; and
- (e) ensuring that your Hosted Content does not require Wavelet to collect, process, or store data in a manner that conflicts with this policy or applicable law.

9 Cookies and Tracking

Wavelet does not deploy cookies or tracking technologies on your services on its own behalf. Any cookies, analytics, tracking pixels, or similar technologies on your services are your responsibility and

are governed by your own privacy notice. Wavelet's own website may use strictly necessary cookies for authentication, session management, and security.

10 Your Rights

As a Client, you have the right to:

- (a) request a copy of the personal information Wavelet holds about you;
- (b) request correction of inaccurate or incomplete information;
- (c) request deletion of your information, subject to legal retention obligations and the terms of any Signed Agreement; and
- (d) request a copy of your data in a commonly used, machine-readable format where technically feasible.

To exercise any of these rights, contact Wavelet in writing at legal@waveletsys.com. Wavelet will verify your identity, typically through your account credentials, and aims to respond within 30 days.

10.1 Jurisdictional Privacy Laws

Although Ohio has not enacted a consumer privacy statute, Wavelet honors the access, correction, and deletion requests described above for all Clients. Where you are a resident of a jurisdiction that does provide privacy rights beyond those above, Wavelet will honor the rights granted by that jurisdiction's law to the extent it applies.

11 Changes to This Policy

Wavelet may update this Privacy Policy from time to time to reflect changes in law, its data practices, or the Services. Material changes will be communicated to Clients by email at least 30 days before the updated policy takes effect. Continued use of the Services after the effective date constitutes acceptance.

12 Governing Law

Except where mandatory data protection law provides otherwise, this Privacy Policy is governed by the laws of the State of Ohio, United States of America. Any disputes relating to this policy shall be resolved in accordance with the governing-law and jurisdiction provisions of the Terms of Service.

13 Contact

Wavelet Systems Ltd
Attn: Legal
6545 Market Avenue N.
North Canton, Ohio, 44721 United States

legal@waveletsys.com