Privacy Policy

Effective date: October 8, 2026 **Last updated:** October 9, 2026

1. Introduction

This Privacy Policy explains how Blue 2 Inc., doing business as Bluehouse Group ("we," "us," or "our"), collects, uses, shares, and protects information in connection with **GeoPeeker** (the "Service"), available at geopeeker.com.

By using the Service, you agree to the practices described in this Policy. If you do not agree, please do not use the Service. Your use of the Service is also governed by our Terms of Service.

Contact: support@geopeeker.com
Mailing address: 193 South Winooski Avenue, Suite 100, Burlington, VT 05401, USA

---

2. Information We Collect

2.1 Information you provide directly

- **Account information**: when you create an account: first name, last name, email address, and a password (stored as a salted hash, never in plaintext). You can also set preferences such as your time zone and date format.
- **Payment information**: paid plans are processed by Stripe. Your card details are entered directly into Stripe's systems and are not stored on or transmitted through GeoPeeker servers. We receive only a customer reference, billing email, and limited metadata (e.g., last four digits, card brand, billing country) from Stripe.
- **Alert contacts**: when you set up alerts, you can add contacts with a name, email address, and mobile phone number. A contact can be you or someone else, such as a colleague. If you add someone else's details, you confirm that you have their permission to do so. See Section 9 (SMS Messaging) for how phone numbers are used.
- **Sites and URLs you submit**: any URL you enter for a peek, an Auto Peek, or a monitor is stored alongside the resulting screenshots, check results, and metadata.
- **Connected services**: if you connect Slack to receive alerts, we store the workspace name, channel name, and the webhook address Slack gives us.
- **Team information**: if you invite people to a Team plan, we store their email address and the status of the invitation.
- **Support requests and communications**: if you contact us, submit a privacy request, or open a support ticket, we retain the contents of your message, any files you attach, and our reply.
- **Product update sign-ups**: if you sign up to hear about product updates, we collect your email address through HubSpot.

2.2 Information collected automatically

When you use the Service (whether or not you have an account), we automatically collect:

- IP address
- Browser type, version, and language
- Operating system and device type
- Referring URL and pages visited within the Service
- Timestamps of requests
- For signed-in sessions, the IP address and browser of each active session
- For API use, a log of each request (endpoint, response status, and response time)

When you run a peek, we collect the URL, the screenshots, and, on plans that include it, the page's HTML source. We also record the site's IP address, the connection time and DNS records seen from each location, and timing and error details for the render. Monitors record their check results, such as status codes, response times, keyword matches, SSL certificate details, and DNS records.

We use cookies and similar technologies for authentication, session management, and analytics. See Section 4 for details.

2.3 Information from third parties

We receive limited information from Stripe (payment events, subscription status), Resend (email delivery, bounce, and spam-complaint events), Vonage (SMS delivery receipts and STOP, HELP, and START replies), and Slack (the workspace and channel you connect), as needed to operate the Service.

---

3. How We Use Information

We use the information described above to:

- Provide, operate, and maintain the Service, including generating peeks and screenshots from your submitted URLs and running the monitors you set up
- Create and manage your account and authenticate you
- Process payments, manage subscriptions, and send billing notifications
- Send transactional emails, verification codes for alert contacts, and the email, SMS, Slack, and in-app alerts you have configured
- Monitor and improve performance, debug errors, and protect the Service against abuse, fraud, and security threats
- Enforce our Terms of Service and comply with legal obligations
- Respond to your support requests. When needed to resolve an issue, authorized staff may view your account as you see it. Each such session is logged.

We do not sell your personal information, and we do not use it for behavioral advertising.

4. Cookies and Analytics

We use a small number of cookies for essential functions: keeping you logged in, protecting forms against cross-site request forgery, and remembering your cookie choice. Stripe's payment script also runs on our pages and may set cookies that Stripe uses to prevent fraud.

We use **Google Analytics** (loaded through Google Tag Manager) and **HubSpot** to understand how visitors use the Service in aggregate. These tools set cookies that collect information such as your IP address, pages viewed, time on page, and approximate location derived from IP. You can opt out of Google Analytics by installing the Google Analytics Opt-out Browser Add-on or by using a browser that blocks tracking.

Visitors in the European Economic Area and the United Kingdom see a cookie banner where they can accept or reject analytics cookies. Google Analytics and HubSpot load only after you click Accept. If you click Reject, they do not load. If we cannot tell where you are visiting from, we show the banner and wait for your choice. To decide whether to show the banner, we look up your approximate country from your IP address using an IP geolocation service and keep the result for one day.

We do not use advertising pixels, retargeting, or A/B testing tools that share data with advertisers.

Most browsers let you control cookies through their settings. Blocking essential cookies may prevent you from logging in or using parts of the Service.

---

5. How We Share Information

We share information only with the service providers ("sub-processors") who help us operate GeoPeeker, and only as needed for that purpose. Each is bound by contract to protect your information and use it only on our instructions.

Sub-processor	Purpose	Location
Amazon Web Services (AWS)	Hosting, file storage (screenshots, page source, support attachments), and the servers used as geo-distributed render nodes	United States and other AWS regions
Cloudflare	Network delivery and security for geopeeker.com	United States and global network
Stripe	Payment processing	United States
Resend	Transactional email delivery	United States
Vonage	SMS delivery (verification codes and configured alerts)	United States
Google Analytics	Aggregate usage analytics	United States
HubSpot	Website analytics and product update emails	United States

Sub-processor	Purpose	Location
Laravel Nightwatch	Application performance monitoring and error tracking	United States
Bunny Fonts	Web font delivery	European Union
ip-api.com	Approximate country lookup for the cookie banner	European Union

We may also disclose information:

- **To people you choose**: members of your team can see your team's sites, peeks, and monitors, and anyone with a share link you create can view that peek's screenshots (see Section 6)
- **To services you connect**: for example, alerts you route to Slack are sent to the Slack channel you chose
- **To comply with law**: in response to a subpoena, court order, or other valid legal process, or where we believe disclosure is necessary to protect rights, safety, or property
- **In connection with a business transaction**: such as a merger, acquisition, or sale of assets, in which case information would transfer subject to this Policy or a successor policy that we will notify you of
- **With your consent**: for any other purpose disclosed to you at the time

We do not sell or rent your personal information to anyone.

---

6. Peek Results and Share Links

Peeks you run while signed in are private to your account and your team. You can make a peek viewable by others by turning on sharing for it. This creates a share link with a long random address. Anyone who has the link can view the peek's screenshots without logging in. The page source is never shown through a share link.

You can turn sharing off at any time from the peek or from the Sharing page in your account, and the link stops working straight away. A share link also stops working when the peek is deleted at the end of its retention period.

Quick peeks run without an account can be viewed only in the browser session that ran them, and they can't be shared. They are deleted after 30 days.

What this means for you:

- The URL and screenshots of a peek you share may be viewed by anyone who has the share link.
- We instruct search engines not to index peek and share pages (via `noindex` directives), but we cannot guarantee that no third party will ever come into possession of a link you share.
- **Do not submit URLs that contain sensitive information** (for example, URLs with authentication tokens, session IDs, password reset links, or private staging credentials in query parameters). Once submitted, the URL and the resulting screenshot are stored, and if you share the peek they are visible to anyone with the share link.

If you need a peek result removed before its normal retention period ends, contact us at support@geopeeker.com.

---

7. International Data Transfers

GeoPeeker is operated from the United States, and the sub-processors listed in Section 5 primarily process data in the United States. If you access the Service from the European Economic Area (EEA), United Kingdom, Switzerland, or another jurisdiction with data-protection laws different from US law, your information will be transferred to, stored in, and processed in the United States.

For transfers from the EEA, UK, and Switzerland, we rely on the European Commission's Standard Contractual Clauses (and, where applicable, the UK International Data Transfer Addendum) with our sub-processors. You may request a copy of the relevant safeguards by emailing support@geopeeker.com.

---

8. Data Retention

We retain information only as long as needed for the purposes described in this Policy or as required by law.

- **Account data**: retained while your account exists. If you cancel a paid plan, your account moves to the Free plan and stays until you delete it. When you delete your account, we delete your account, sites, peeks, monitors, alert contacts, and connected services straight away. Two things are kept: your support tickets, and your customer record with Stripe, which we keep for accounting purposes only. Backups containing the data are overwritten on our standard rotation.
- **Peeks and screenshots**: retained for the period your plan allows: **30 days** on Free, **60 days** on Solo, **90 days** on Pro, and **365 days** on Team and Enterprise. Quick peeks run without an account are kept for 30 days. Peeks are deleted automatically when the period ends.
- **Monitoring history**: uptime and keyword check results and resolved alerts are kept for **30 days**. DNS and SSL history is kept while the site is in your account.
- **Server and application logs**: retained for up to **90 days** for security, debugging, and abuse-prevention purposes. API request logs are kept while your account exists.
- **Support tickets**: retained as a record of the request and our response, including after you delete your account.
- **Email suppression list**: if an email to you bounces or you mark one as spam, we keep the address on a suppression list so we do not email it again.
- **Payment and tax records**: your Stripe customer record and payment history are retained for accounting purposes only, for as long as required by applicable tax and financial-recordkeeping law (typically 7 years in the United States), even after account deletion.
- **SMS opt-out records**: retained so that we do not message a number that has opted out (see Section 9).

9. SMS Messaging (Verification Codes and Alerts)

If a mobile phone number is added to an alert contact in GeoPeeker and opted in to SMS, the following terms apply.

Types of messages. A number receives SMS only for these categories:

- **Verification codes**: a one-time code that confirms the number when the contact is added
- **Monitor alerts**: alerts that the account holder has set up for monitored sites

We do not send marketing or promotional SMS.

How phone numbers are collected. A phone number is entered on an alert contact in the account's settings, and the person adding it must check an unchecked consent box before any messages are sent. Providing a phone number is optional. Alerts can also go by email, Slack, or in-app notification.

Frequency. Message frequency varies. On average, contacts with alerts configured receive a handful of messages per month. Verification codes are sent only when a phone number is added or changed, or when a new code is requested.

Cost. Message and data rates may apply, as set by your mobile carrier.

Opt-out. You can opt out at any time by replying **STOP** to any GeoPeeker SMS. You will receive a single confirmation message and will not receive further SMS unless you opt back in by replying **START** or through account settings. Reply **HELP** for help, or contact support@geopeeker.com.

Carrier disclaimers. Carriers are not liable for delayed or undelivered messages.

Sender. Messages are sent from "GeoPeeker" via our SMS provider, Vonage.

No sharing of mobile information for marketing. No mobile information will be shared with third parties or affiliates for marketing or promotional purposes. All categories of personal information described in this Policy exclude mobile phone numbers, SMS opt-in data, and SMS consent records. **This information will not be shared with any third party for marketing or promotional purposes.** It is shared only with Vonage solely to deliver the messages requested, and as required by law.

---

10. Your Privacy Rights

10.1 Rights for individuals in the European Economic Area, United Kingdom, and Switzerland (GDPR)

If you are located in the EEA, UK, or Switzerland, you have the following rights regarding your personal data:

- **Access**: request a copy of the personal data we hold about you
- **Rectification**: request that we correct inaccurate or incomplete data
- **Erasure** ("right to be forgotten"): request deletion of your data, subject to certain exceptions

- **Restriction**: request that we limit how we process your data
- **Portability**: request a copy of your data in a structured, machine-readable format
- **Objection**: object to processing based on our legitimate interests
- **Withdraw consent**: where processing is based on consent (e.g., SMS opt-in or analytics cookies), withdraw it at any time

Legal bases for processing. We process your data under one or more of the following GDPR legal bases: performance of a contract (operating your account and the Service), legitimate interests (security, fraud prevention, improving the Service), consent (SMS, analytics cookies, marketing communications you've opted into), and legal obligation (tax and recordkeeping).

To exercise any of these rights, use our privacy request form or email support@geopeeker.com. You also have the right to lodge a complaint with your local data-protection authority.

10.2 Rights for California residents (CCPA/CPRA)

If you are a California resident, you have the right to:

- **Know** what personal information we collect, use, disclose, and (if applicable) sell or share about you
- **Access** the specific pieces of personal information we have collected about you in the prior 12 months
- **Delete** personal information we have collected from you, subject to certain exceptions
- **Correct** inaccurate personal information
- **Opt out** of the sale or sharing of personal information: **we do not sell or share personal information as those terms are defined under California law**
- **Limit the use of sensitive personal information**: we do not use sensitive personal information beyond what is necessary to provide the Service
- **Non-discrimination**: we will not discriminate against you for exercising any of these rights

To exercise these rights, use our privacy request form or email support@geopeeker.com. We may need to verify your identity before processing the request. You may also designate an authorized agent to make a request on your behalf.

10.3 Other US state privacy laws

Residents of Virginia, Colorado, Connecticut, Utah, and other states with comprehensive consumer-privacy laws may have rights similar to those described above. Use our privacy request form or email support@geopeeker.com to exercise them.

10.4 How to submit a request

Submit a request to access, delete, correct, or export your data through our privacy request form, or email support@geopeeker.com. You do not need an account to make a request, and you can make one through an authorized agent. We may need to verify your identity before fulfilling a request. If you are signed in, you can also delete your account straight away from your account settings. We respond to verified requests within the timeframes required by applicable law (generally 30–45 days).

11. Children's Privacy

The Service is intended for web and technology professionals and is not directed to children under 16. We do not knowingly collect personal information from children under 16. If you believe a child has provided us with personal information, please email support@geopeeker.com and we will delete it.

---

12. Security

We use industry-standard technical and organizational measures to protect your information, including:

- TLS encryption for data in transit
- Passwords and verification codes stored as one-way hashes
- Encryption at rest for stored files
- Restricted access to production systems on a need-to-know basis, with staff access to customer accounts logged
- Logging and monitoring via Laravel Nightwatch for anomaly detection, with passwords, tokens, and cookies removed before they are recorded
- Use of vetted sub-processors (AWS, Cloudflare, Stripe, Resend, Vonage) that maintain their own enterprise security programs

No method of transmission or storage is perfectly secure. We cannot guarantee absolute security, but we work to protect your information and will notify affected users and regulators of any breach as required by law.

---

13. Changes to This Policy

We may update this Policy from time to time. When we do, we will revise the "Last updated" date at the top and, for material changes, provide additional notice (such as a banner on the Service or an email to account holders). Your continued use of the Service after the changes take effect constitutes acceptance of the updated Policy.

---

14. Contact Us

Questions, requests, or complaints about this Policy or our privacy practices:

Blue 2 Inc. (dba Bluehouse Group)
193 South Winooski Avenue, Suite 100
Burlington, VT 05401
USA
Email: support@geopeeker.com