

PRIVACY POLICY

Latest Update: March 2026

This Privacy Policy explains how Flare Systems, Inc. ("Flare") collects, uses, and protects your personal data when you use our services for personal purposes, including VIP Protection. This includes situations where access is provided through your employer or another organization.

It also explains how we process personal data to develop our services and provide cybersecurity intelligence capabilities, as well as your privacy rights and how to exercise them.

If you have any questions or wish to exercise your rights, you can contact us at any time.

Flare Systems, Inc.
Attention: Privacy Officer/Data Protection Officer
1751 rue Richardson, Unit 3,108
Montréal, Quebec, H3K 1G6
1-833-685-3527
privacy@flare.io

Flare also provides cybersecurity services for organizations, including cyber threat intelligence and threat exposure management. These commercial services are covered by the [Flare Platform Privacy Notice](#). Information about how we process personal data on our website, including marketing and recruitment activities, is available in our [Website Privacy Notice](#).

If you are located in the European Union or the United Kingdom, Flare acts as the data controller for the personal data processed through these services. This means we determine how and why your personal data is processed when you use Foretrace.

PERSONAL DATA COLLECTION

We process personal data for the following purposes:

- to collect and organize threat and exposure information
- to develop and improve our services
- to provide our services to you

Depending on your location, we rely on different legal bases for this processing, including the performance of a contract, your consent, or our legitimate interests.

To conduct research and development

We process data to improve our detection, classification, and remediation capabilities for cybersecurity threats. For this purpose, we use:

- intelligence data relating to cybersecurity events and threats (such as compromised identifiers, incident metadata, and threat actor techniques and patterns), and
- limited technical data, such as system performance information.

We use automated tools and algorithms within our systems to develop and improve detection and classification models. This includes classifying alerts, identifying threat patterns, assigning risk levels, and organizing information to provide relevant and contextualized security insights.

These models operate on intelligence data within our systems and do not use your activity, your use of the service, or data from your environment.

To collect and organize threat exposure information

To provide cybersecurity services, Flare collects and processes information from third-party sources, including websites, forums, and sources where information about cyber incidents may be published.

We organize and index this information so it can be searched using identifiers such as an email address or domain. This processing occurs regardless of whether you create an account.

This information (referred to as “intelligence data”) may include personal data that has been publicly exposed or shared in connection with cybersecurity incidents, such as:

- email addresses or usernames
- leaked credentials
- contact or financial information
- data appearing in breach datasets or similar sources

We may store limited extracts of this information or references that allow the original source to be retrieved. This data is not linked to your account when collected. It is only associated with you when you verify an identifier and choose to use the service.

If you are located in the European Union or the United Kingdom, we process personal data for this purpose based on our legitimate interests, or those of the organizations that use our services. These interests include detecting and monitoring cybersecurity threats, helping individuals and organizations understand and reduce exposure risks, and supporting the prevention of cybercrime.

To provide our services to you

We process personal data to provide VIP Protection and other services you choose to use.

Depending on your location, this processing is based on your consent or on the performance of a contract. You may withdraw your consent at any time by deleting your account or contacting us.

To provide the service, we process:

- your corporate email address used to create and verify your account (the domain must be authorized by the sponsoring organization)
- additional email addresses you choose to monitor as identifiers
- exposure data linked to those identifiers

Once your email address is verified, VIP Protection retrieves and displays exposure information associated with that identifier in your dashboard. This may include:

- the source of the exposure
- the date and type of incident
- the categories of data involved

This information may include data that has already been publicly exposed during cybersecurity incidents.

PERSONAL DATA WE RECEIVE FROM THIRD PARTIES

We may collect personal data about you from third-party sources, including publicly accessible websites, forums, social media platforms, and breach datasets where information related to cybersecurity incidents may appear.

This may include personal data associated with identifiers such as an email address. We use this information to identify potential exposure risks and provide visibility into data that may already be available online.

Organizations using the Flare Platform may also provide identifiers they manage (such as corporate email addresses) to monitor potential security exposures. In these cases, we process personal data on their behalf and only for that purpose.

PERSONAL DATA WE SHARE WITH THIRD PARTIES

We share personal data only where necessary to provide our services. We do not sell personal data or use it for marketing or cross-context advertising.

Organizations providing your access

If your access is provided by an organization (such as your employer), that organization may receive limited account-related information, such as whether your account was activated. It does not have access to your personal dashboard or exposure data.

Organizations using our cybersecurity services

We also provide cybersecurity intelligence services to organizations. This may include information linked to identifiers (such as email addresses) that appears in breach datasets or other cybersecurity-related sources. These organizations are required to use the service only for assets they are authorized to monitor.

Service providers

We rely on a limited number of service providers to operate our services. These providers process personal data on our instructions and are required to protect it.

Legal and security purposes

We may disclose personal data if required by law or where necessary to help prevent or investigate cybercrime. We do not normally share your account data unless legally required, but we may share information collected through our threat intelligence activities.

Corporate transactions

If Flare is involved in a merger or similar transaction, personal data may be transferred as part of that process.

PROFILING AND AUTOMATED DECISION MAKING

When you use our services, we analyze exposure data linked to a validated identifier (such as your email address) to generate a personal exposure profile. This may be considered profiling under applicable privacy laws.

This includes:

- a history of exposure events
- risk indicators and security scores based on objective factors such as the number, type, and timing of exposures

This processing is performed at your request and is based on objective data, not your behaviour or activity. It does not involve automated decision-making that produces legal or similarly significant effects.

Your exposure profile is not shared with your employer or third parties and is not used for marketing, behavioural profiling, or tracking.

COOKIES AND TRACKING TECHNOLOGIES

We do not use cookies for advertising, marketing, or cross-site tracking. We use the following types of cookies:

- **Essential Cookies:** These cookies are necessary for the service to function properly. They support secure login, session management, and protection against security threats. Without them, the service cannot operate correctly.
- **Functional Cookies:** These cookies help remember certain settings and preferences within the service, such as language or configuration choices.
- **Analytical Cookies:** We use limited analytics tools, such as Pendo, to understand how features are used and to improve the reliability and usability of our services. This analytics is used only to improve the service and do not involve advertising tracking or behavioural profiling across websites.

You can manage or block cookies through your browser settings. Most browsers allow you to review and delete cookies at any time. Please note that blocking certain cookies may affect the availability or security of some features of the service. Instructions for managing cookies are available for common browsers:

- [Google Chrome](#)
- [Firefox](#)
- [Safari](#)
- [Microsoft Edge](#)
- [Opera](#)
- [Brave](#)

SECURITY SAFEGUARDS

We implement technical and organizational measures designed to protect personal data and limit unauthorized access.

These measures include access controls restricting data to authorized personnel, ongoing system monitoring and security testing (including vulnerability scanning and periodic independent testing), and processes to identify and remediate vulnerabilities through patching and updates.

We also apply secure development practices, encryption, and system safeguards to protect data in our systems and during transmission. Our personnel receive training on security threats such as phishing and social engineering, and we maintain a formal security program supported by risk assessments and internal policies.

Our security controls are independently assessed as part of a SOC 2 Type II attestation. Additional information is available in our [Trust Center](#).

DATA STORAGE AND INTERNATIONAL TRANSFERS

Flare's systems are hosted in **data centres located in the United States**, and our services, including technical support, are primarily provided from **Canada**.

Some of the information processed through our services comes from **sources located around the world**, such as websites, forums, social media platforms, or breach datasets where information related to cybersecurity incidents may appear. In many cases, this information has already been made public online or shared in criminal forums before it is identified through our monitoring activities.

Flare does **not control these original sources or where they are hosted**. We may collect, index, or store limited information from them so that exposure data can be identified and displayed through our services, while the original content remains hosted by third parties.

When we share personal data with service providers, organizations, or clients in order to provide our services, we use **appropriate contractual and technical safeguards** designed to protect personal data.

When personal data is stored or processed outside the country where you are located, it may be subject to the laws of those jurisdictions, which may allow government authorities to access the data under certain circumstances.

DATA RETENTION

We retain personal data for as long as necessary to fulfill the purposes described in this Privacy Policy, or longer where required by law.

Personal data related to your account, such as your email address, is retained for as long as your account remains active.

ACCOUNT DELETION

If your account is deleted, the information associated with it is also deleted. This includes identifiers (such as your email address), linkage data, and usage data.

To request deletion, you may contact the organization that provided your access or contact us directly. Some services may also include built-in features to request account deletion.

If your access was provided by an organization, that organization is responsible for managing your account and handling related requests. It should be your primary point of contact for account-related matters.

INDIVIDUAL RIGHTS

Depending on your location, you may have rights over your personal data, including the right to access, correct, delete, or receive a copy of your data, and to object to or restrict certain processing.

In the European Union and the United Kingdom, your rights include:

- The right to be informed about how we process your personal data.
- The right to access your personal data.
- The right to rectify personal data, such as if it is inaccurate.
- The right to request the erasure of your personal data.
- The right to request the portability of your personal data.
- The right to object to the processing of your personal data.
- The right to contest automated decision-making.

You can read [this guide](#) from the UK'S Information Commissioner Office for more information.

If you decide to exercise your rights, we may need to ask for additional personal data about you so that we can identify you prior to responding to your request. If we can't comply with your request, we will explain why. We will get back to you within the delays required by applicable laws to your request.

You have the right to lodge a complaint with a data protection authority in your country of residence or place of work.

If you are in Canada, you can reach out to the Office of the Privacy Commissioner on their website at www.priv.gc.ca.

CAN WE MODIFY THIS PRIVACY POLICY?

Yes, we can modify this Privacy Policy as necessary, such as to reflect our current processing of personal data or to new legal requirements. When we modify this policy, we will notify users through their emails or via the application and update the date at which this document was updated above.