PRIVACY POLICY

Latest Update: October 14, 2025 - Version 2.5

This Privacy Policy is intended to provide you with information on how we collect, use, and disclose personal data as part of our commercial services, click here for more information on the scope of this Privacy Policy. To learn more about our other processing of personal data, click here.

It contains information on your rights regarding your personal data, and how you can exercise them. If you have any questions on this Privacy Policy, or otherwise to exercise your rights, you can reach out to us at any time. We will try our best to assist you:

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

1. WHAT IS THE SCOPE OF THIS PRIVACY POLICY?

This policy applies to your use of the Flare Platform and related threat intelligence services, including:

- Platform hosting, maintenance and user account management
- Delivery of intelligence data and monitoring of selected identifiers or corporate identities
- Retrieval and analysis of public and dark web content for threat detection
- Technical support and processing of takedown requests

(The "**Services**")

The "dark net" or "dark web" refers to hidden online networks and forums, which are sometimes used for selling or acquiring illegally corporate and personal data, as well as for other illicit activities.

Our Services are intended to help organizations detect and prevent fraud, protect their information assets, monitor digital risks, and lawfully collect and analyze threat intelligence from public and other sources.

We maintain contractual agreements with our clients that restrict their use of the Flare Platform to lawful and authorized purposes. Our clients may include managed security service providers and other organizations offering threat intelligence, digital forensics, threat detection, or related security services. To understand how your personal data is processed as part of their services or their use of the Flare Platform, please contact the relevant client directly.

We are a data processor when we provide the Services by processing personal data on behalf of our clients unless specifically indicated otherwise in this policy.

2. WHAT PERSONAL DATA DO WE COLLECT AND FOR WHAT PURPOSES?

To offer and manage the Flare Platform, we collect personal data directly from the users, as well as from our clients. The Services also involve the processing of personal data obtained through third-party sources, including by indexing content from public sources that can include personal data.

This content can be searched for threat intelligence purposes using identifiers configured on the Flare Platform. Examples of identifiers include domain names, keywords, executive names, employees' e-mail and IP addresses. Our clients are responsible for informing individuals of the personal data collected about them when they use the Services.

If we process your personal data based on your consent, you can withdraw this consent at any time at privacy@flare.io, or through the functionalities made available to you.

Purposes of Processing	Types of Personal Data
To create and manage user accounts	We collect the following types of personal data to manage accounts: ● Credentials ● E-mail address ● Team members ● Collaborators ● Name of employer
To respond to take down services requests from users	When using our services, users can make requests to take down domains and other digital assets. To respond to these requests, we will have access to the user data (name, nature of requests). We may also exchange communication and may access other personal data to proceed with the request.
To provide query results to users and provide threat intelligence on the results obtained	Using our search bar, users can search for content relating to their queries on monitored sources, including the dark net. The information shared with users can include personal data of individuals. The search bar also generates usage data when used. We use AI to analyze threat intelligence data and provide additional contextual information to help users understand the information that they obtain from the queries.
To retrieve content from monitored sources, including the dark web	Users can request access to the monitored content annexed in the platform, such as a file from the dark net. Flare does not inspect or scan the content retrieved, and we do not know what it contains. Retrieved content can include different types of personal data, including stolen or leaked credit card numbers, credentials, and social security numbers. It can also include posts on public forums, as well as their content and reactions by users.
For the monitoring of identifiers to detect security incidents, fraud and other threats	Identifiers are used for the monitoring of assets, and the creation of related alerts. Our clients can choose different types of identifiers, many of which can allow the monitoring of individuals, including to profile risks. The Flare Platform can provide alerts to users about the content found in relation to these identifiers.
To monitor corporate identities for exposure events	If users integrate with an authorized identity management system (e.g., through Entra ID), they can create corporate identifiers to monitor the use of corporate accounts and services across their controlled identifiers. We collect work e-mail addresses, department names, and job titles synchronized by the customer, along with exposure information obtained from monitored sources about the corporate accounts to create these profiles. And obtain alerts about security events.

To offer alerting services related to monitored identifiers	To receive alerts on monitored content, users must provide their e-mail addresses and select the frequency at which they want to receive communications. These settings can be modified at any time in the platform.
To provide threat intelligence to organizations based on identifiers	We index and match publicly available and dark web data, including stealer log content, to identifiers selected by our clients for authorized purposes such as fraud prevention and cybersecurity monitoring. We do not control this content or the personal data it may contain. The Flare Platform monitors relevant sources to help clients detect data breaches and respond to fraud or cyberattacks. Examples of data that may appear in these sources include email addresses, usernames, passwords, credit card numbers, or government identifiers.
For security purposes, including user authentication	We process personal data such as usernames, email addresses, passwords, credentials, and usage data (including session information, user preferences, and authentication tokens). The Flare Platform also collects IP addresses, device details, browser type, operating system, and system logs. These data points may be aggregated and analyzed to establish correlation rules based on user behaviors and actions.
To allow organizations to validate passwords reuse across service accounts	Corporate services account passwords are not displayed in plain text within the Flare Platform. Certain functionalities allow organizations to identify when corporate passwords have been reused, helping protect their networks and authenticated identifiers (for example, through an identity management system) linked to professional service accounts. Corporate profiling features do not provide visibility into employees' personal passwords or other validated identity credentials.
For consent and preferences management	The Flare Platform stores user preferences and consent details, including consents provided, their timing, and account settings such as language. To support this functionality, the platform collects certain technical data such as browser type, IP address, and device information.
To respond to technical support requests	We collect personal data such as your name, email address, the content of your requests, any attachments, and related actions when you submit a support ticket.
To improve the Flare Platform, including to resolve bugs and increase performance	We use usage data to understand how the Flare Platform is performing and to improve our functionalities, including our machine learning models. This includes device and browser information, IP addresses and usage logs. This personal data used for this purpose may also include aggregated data and usage data.

3. ARE THERE ANY COOKIES USED AS PART OF THE SERVICES?

We use some cookies as part of our Services. We don't conduct interest-based marketing through our Services, and we don't use marketing or remarketing cookies.

Type of cookies	Description
Essential Cookies	Essential cookies are necessary to operate the core functions of our websites. These include login cookies, session ID cookies, language cookies as well as security cookies.
Functional Cookies	Functional cookies are used to provide you with certain website functionality, and to remember website preferences, consents, and configurations. For instance, when providing support, we may use cookies to help us track requests in association to users.

Analytical Cookies	Analytical cookies are used to generate aggregated statistical data about traffic and behaviour of our users. For instance, Pendo may use cookies from time to time, such as in older browsers, so that it can provide us with user behaviour statistics which we use to manage our platform and improve our Services.

4. HOW CAN YOU MANAGE YOUR COOKIE PREFERENCES?

You can manage your cookie preferences through your browser, by uninstalling and blocking certain cookies. Click on your browser below to obtain instructions. You can withdraw your consent on the use of cookies at any time by managing your preferences. Certain features may require cookies for security purposes.

- Google Chrome
- Firefox
- Safari
- Microsoft Edge
- Opera
- Brave

5. DO WE SHARE YOUR PERSONAL DATA WITH THIRD PARTIES?

We share personal data to provide the Services, including to service providers, and our clients who access personal data for security and fraud prevention purposes. We do not use your personal data for marketing.

There are a few other cases when we can share your personal data, if we reasonably believe we have to, or if we believe it is necessary for security purposes.

- As part of a commercial transaction, e.g., to a potential acquirer
- Upon request from the authorities, e.g., a court order
- To prevent harm to individuals, e.g., to the authorities

We may proactively share personal data with the authorities or law enforcement if we believe that it can help reduce cyber criminality and prevent further harm to individuals.

Categories	Additional information
Service Providers	We use service providers to provide you with information technologies. We use Amazon Web Services as a cloud hosting company for the Flare Platform, and SendGrid for the communication functionalities within the Flare Platform. We also use service providers to obtain analytics services on the usage of the Flare Platform, such as Pendo, to manage its performance.
Integration Partners	Our platform can be integrated with third-party services, platforms and applications based on how our clients configure the use of their Services. This can result in the disclosure of personal data from the Flare Platform to a third party's environment. Typical integrations involve sending event alerts from the Flare Platform to a technology platform used by your organization. Examples of this could include an alert sent to your organization's Slack or Microsoft Sentinel

Categories	Additional information
	environments. While these integrations are enabled by our clients, the integration may involve the disclosure of personal data such as username, e-mail address, or other personal data to this third party. You can learn more about our integration ecosystem here.
Clients	Our clients access personal data indexed through the Flare Platform by using search, query and monitoring functions. They can also extract personal data with the retrieval function.

6. HOW DO WE PROTECT PERSONAL DATA?

We implement reasonable technical and organizational measures to protect personal data. Our security program is subject to a SOC 2 Type II attestation, confirming controls operated effectively throughout the reporting period. Here are some of the safeguards that we maintain:

- **Encryption.** All data stored in the Flare Platform is encrypted at rest and in transit using industry-standard protocols.
- **Security Testing.** We perform intrusion testing of the flare Platform to identify and remediate potential vulnerabilities.
- **Incident Preparedness.** We maintain an incident response plan and a business continuity program to ensure we respond effectively to security events and maintain service availability during disruptions.
- **Access Control.** We apply role-based access controls and grant access to personal data only to authorized personnel who require it for their role.
- **Trusted Infrastructure.** The Flare Platform is hosted in a data centre that undergoes independent audits for norms such as ISO 27001, ISO 27017 and ISO 27018.

7. WHERE DO WE STORE YOUR PERSONAL DATA?

We host our Services on a cloud in the United States, and some of our Service Providers may also be in the United States. Your personal data are encrypted at rest and in-transit, including when hosted by our service provider. When stored in another country than the country in which you are located, your personal data may be subject to different laws, which may permit, under certain circumstances, access by governmental entities. If we receive such a request, we will try our best to let you know before complying unless we can't do so.

8. HOW LONG DO WE RETAIN YOUR PERSONAL DATA?

We retain user account personal data, such as credentials for as long as they have an active account with us. Our clients can provision and delete inactive accounts or may request the deletion of such accounts directly with us. When our service agreements with our clients are terminated or are expired, we delete users' personal data in accordance with such agreements.

Corporate identities created through integration with partners are kept active for as long as the identity exists in the source system, or if the source system indicates this identity must be monitored. Our clients control whose identities are monitored. Once an identity is no longer monitored, the data related to this identity is no longer associated with the identity, and the profile information is deleted.

We keep personal data for as long as required for the purpose of processing and in certain circumstances, we must retain the personal data longer to comply with the law.

9. DO WE USE PROFILING TECHNOLOGIES AND AUTOMATED DECISION-MAKING?

We do not permit the use of our Services to unlawfully profile individuals or otherwise infringe on their privacy rights. Our clients are responsible for ensuring their use of the Flare Platform complies with applicable laws, including any requirements to inform individuals of such activities.

The Flare Platform includes limited profiling and automation features, as described below:

- **Fraud prevention and monitoring.** Clients may use the Platform to monitor individuals or entities for legitimate security purposes, such as preventing fraud or identifying compromised credentials.
- **Corporate identity monitoring.** Clients can connect the Platform to their identity or employee management systems to create corporate profiles and monitor exposure of related accounts.
- **Automated analysis.** Certain features perform limited automated matching to identify potential data exposures. These do not involve behavioural profiling or automated decision-making.

While the Flare Platform uses artificial intelligence, it is used to provide non-binding contextual information on the results obtained from queries and monitoring services, and not for automated decision-making. Clients must verify the intelligence data provided through the Flare Platform solely to help the user understand the results.
Personal data associated with these profiles is stored in the United States. We do not currently offer multi-jurisdictional data hosting.

This notice describes the current functionalities and permits uses of the Flare Platform. We strive to implement safeguards to ensure the platform operates in accordance with our acceptable use requirements.

10. WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?

Privacy laws worldwide provide you with different rights over your personal data. These rights can include the right to deletion, to data portability, to be informed of our processing of your personal data, and to withdraw your consent. Our Privacy Officer will respond to your request within 30 days or will inform you of the motives if your request is denied.

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.

Please let us know if you have any concerns or complaints about how we process personal data by reaching out directly with our Privacy Officer. We will handle your complaint seriously and take the required actions.

If you are still not satisfied, you can also contact your local regulator to understand how to make a complaint. If you are in Canada, you can reach out to the Office of the Privacy Commissioner on their website at www.priv.gc.ca.

11. 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 our users as required under the law. You can see the latest date at which we updated this Privacy Policy at the top of this page.