# Privacy Policy

Version 2.3: 12 June 2023

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
Montreal, Quebec,  H3K 1G6
1-833-685-3527
privacy@flare.io

## 1. WHAT IS THE SCOPE OF THIS PRIVACY POLICY?

This policy covers our threat intelligence services and your use of the Flare Platform, including:

- The hosting and maintenance of the Flare Platform.
- The provision of intelligence data through data analytics.
- Your use of the search bar to consult public content for threat indications, including on the dark web, and the indexation of public content for this purpose.
- User account management.
- The monitoring of identifiers selected by our clients.
- The retrieval of content from the dark net.
- The provision of threat intelligence monitoring services.
- The provision of technical support services.
- The processing of takedown requests of domains and other digital assets.

(The “**Services**”)

The “dark net” ou “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 for fraud prevention, information security, the acquisition of threat intelligence, and other lawful purposes. We have contracts in place with our clients that restrict their use for legal purposes. Our clients may include managed security services provided providers, who are providing threat intelligence monitoring, digital forensic, threat detection and similar services. Please reach out to our clients to understand how they process your personal data, either as part of their services, or as part of their use of the Flare Platform.

By personal data, we mean any data that can directly or indirectly identify an individual, like a user of the Flare Platform. Some of the personal data that we cover in this policy may not benefit from legal protection, and you may not have the same rights as explained in this policy over such personal data.

This policy does not apply in these circumstances:

- Processing of non-personal data such as de-identified and aggregated data. These data don't allow us to identify anyone.
- Third-party websites, applications, services, and products, even if these are linked or can be integrated into our Services.

We are a data processor when we provide the Services by processing personal data on behalf of our clients.

## 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:<br>● Credentials<br>● E-mail address<br>● Team members<br>● Collaborators<br>● 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.<br>We use artificial intelligence 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 | The Flare Platform contains a functionality allowing users to request access to the content available through a monitored source, such as the dark net. When complying with a retrieval order, Flare does not inspect or scan the content retrieved, and we do not know what it contains. Only clients can make this analysis. |

| **Purposes of Processing** | **Types of Personal Data** |
|---|---|
| | 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 manage alerts relating to monitoring activities | Clients can configure the Flare Platform to issue alerts regarding identifiers. If so, we will collect the information required, such as the e-mail addresses for the alerts, as well as the frequency of the alerts. |
| To make our threat intelligence services available | To allow organizations to effectively search intelligence data, including personal data leaked on the dark net, we process this content by indexing it. This indexing is only for authorized purposes, such as fraud prevention.<br>We do not control this content, nor what types of personal data may be included. We monitor sources that are relevant to threat intelligence, including public-facing interfaces for evidence of data breaches. Threat intelligence allows our clients to take immediate actions and limit damages resulting from fraud and cyberattacks. Depending on the search queries, clients can access any personal data available through the monitored sources, including stolen credit card numbers, leaked social insurance numbers, and suspicious conversations on forums frequently used for criminal activities, the whole in relation to stakeholders for whom they provide threat monitoring services.<br>Our clients can also buy service credits that they can exchange for personalized reports and services regarding threat intelligence. |
| For security purposes, including to ensure a secure authentication process to the Flare Platform | For security purposes, we process personal data such as usernames, e-mail addresses, passwords, credentials, usage data (session information, user preferences, and authentication tokens, allowing the application to recognize and validate users during subsequent visits).<br>The Flare Platform collects IP addresses and device information, such as browser type and operating systems, as well as logs, audit trails, recording user activities, login attempts, and system events. |
| For consent and preferences management | To provide the Services, we have to remember some parameters when users access their accounts, such as:<br>● Consents received<br>● Timing of consents<br>● Account preferences, such as language<br>The personal data collected to help us remember preferences include:<br>● Browser type<br>● IP address |

| **Purposes of Processing** | **Types of Personal Data** |
|---|---|
| | ● Device information |
| To respond to technical support requests from users | We collect personal data to respond to support tickets, e.g., your name, e-mail address, and the content of your requests, as well as related actions. |
| 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. |

## 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.<br>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.<br>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 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 associated with an alert. 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 your personal data, such as policies. Here are a few examples:

- We use AES 256 encryption at rest and AES128 or AES 256 for encryption in transit for all data transfer to or from the Flare Platform.

- We perform end-to-end internal penetration testing of our Flare Platform.

- If something should go wrong, we have an incident response plan prepared to handle a security breach. We also have a business continuity plan to make sure that we can maintain our availability and respond to natural disasters.

- We have a strong role-based access system mechanism, and we only provide access to data on a need-to-know basis.

Our cloud hosting company complies with many security standards, and is audited by third parties for ISO 9001, ISO 27001, ISO 27017 and ISO 27018. They also have SOC 1/ISAE 3402, SOC 2 and SOC 3 reports.

## 7. WHERE DO WE STORE YOUR PERSONAL DATA?

We host our Services on Amazon Web Services 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 Amazon Web Services. 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 personal data of users 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. We keep personal data for as long as required for the purpose of processing but 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?

It is possible to use the Flare Platform to monitor individuals to prevent fraud. We do not allow the use of our Services to profile individuals unlawfully, including in breach of their privacy rights. Our clients must comply with applicable laws when they use the Services, including by communicating such practices with concerned individuals.

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.

## 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 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’ll try our best to get back to you in 30 days, or we will let you know if we need more time.

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.