

WEBSITE PRIVACY STATEMENT

Latest Update: **January 1st, 2024**,
Version 0.1 – this is a pre-release preview

This Website Privacy Statement contains information on how we process your personal data through our website and digital activities, including the types of personal data we collect and for what purposes, with whom we share your personal data as well as the rights that you can exercise regarding your personal data. [Click here](#) to learn more about what is included in this statement.

Please review our [Services Privacy Statement](#) for more information about how we process your personal data as part of our professional services.

We named a Privacy Officer to oversee the processing of your personal data and manage our privacy compliance program. If you have any questions related to your privacy, would like to exercise your rights, or have any complaints regarding our processing of your personal data, please reach out to our Privacy Officer.

By e-mail at: privacy@henriwolf.law

If you're more of the traditional type, you may reach out to our Privacy Officer by mail at the following address:

Henri & Wolf, Inc.

At the attention of: Privacy Officer
731 De la Commune St W, Bureau 100
Montreal, Quebec
H3C 1X7, Canada

As part of our digital advertising activities, we use targeting capabilities available through platforms such as LinkedIn and Google Ads. We do not perform any retargeting as part of our professional or legal services. We seek to comply with the guidelines from the [Digital Advertising Alliance](#) regarding enhanced disclosures. [Click here](#) to learn more about our use of targeting.

This page uses a Q&A format, click on each question to learn about each topic. You will be provided with a summary or overview of the response. You also have the option to expand some responses to dive in a topic that is of interest. If you don't find what you're looking for, you can also message us at privacy@henriwolf.law.

1. What is the scope of this Website Privacy Statement?

This statement applies to our online activities, including:

- When you navigate our website, including any comments you may leave.
- If you purchase products through our [Knowledge Center](#).
- If you subscribe to a paid subscription, including to [The Monitor](#).
- When you communicate with us, including by filling in a form on our website.
- Our management of our website's performance and analytics.

- Our digital advertising and marketing activities.
- When you download a whitepaper or resources that we make available to you.
- If you subscribe to or participate in an event that we are organizing, such as a webinar.
- If you contact us regarding our community, including by sharing your resume.
- If you comment on a blog or piece of content open for public comments.
- To ensure the security of our website, including when we process a payment.

Our processing of personal data pursuant to our products and services, including commercial subscriptions to our legislative monitoring newsletters, The Monitor, is subject to the Services Privacy Statement.

This statement does not apply to third-party services, applications, and products. If you decide to share content using a social media widget, or if you decide to save your personal data through Stripe to use it across merchants, these data processing components are not covered by this privacy statement. Make sure that you read the applicable policies before using these third parties.

[Click here for more information.](#)

This policy outlines our approach to managing personal data. The interpretation of "personal data" can differ based on applicable law, and it may not fully include business contact details. In this context, "personal data" refers to any information, which alone or combined with other information, can identify an individual, irrespective of the legal protections in place. Therefore, your rights may vary across different types of your personal data, but we are committed to helping you exercise your rights, nonetheless.

Cookies, along with other tracking technologies, are small files stored on your device when you use the internet or certain applications. They originate from websites and are retained by your web browser. Their functions range from remembering your preferences, facilitating efficient navigation, improving user experience, to being utilized in digital advertising. For an in-depth understanding of cookies, other tracking technologies, and our practices in digital advertising, please refer to the relevant sections.

[2. What personal data do we collect about you, and for what purposes?](#)

We collect personal data directly from you, such as if you enter your contact information in a form, or your payment information when you subscribe to an online service, such as our legislative monitoring newsletters, The Monitor, or purchase a product from our Knowledge Center. If you are provided with access to our subscriptions, services or products through a third-party organization, this organization provided us with your business contact information as part of our commercial services.

We also collect data automatically through our website, including your IP address, the dates and time at which the website or a page is accessed, and your geolocation. We do not collect precise location information.

We do not purchase data about you from third parties. We engage in some targeting based on professional qualifications and interests. [Click here](#) to learn more our use of cookies and [click here](#) to learn more about our digital advertising practices.

We generally process your personal data based on your consent. You can withdraw that consent at any time. [Click here](#) to learn how to manage your consent regarding cookies. At all times, you can also write to us at privacy@henriwolf.law.

[Click here to learn more.](#)

Below is a detailed overview of the purposes for which we collect personal data, along with examples of personal data collected for each purpose.

Purposes	Explanations
<p>To manage subscriptions to our newsletters, including if you want to unsubscribe.</p>	<p>From time to time, we may offer different newsletters, including paid subscriptions. If you decide to subscribe to these services, you will have to register by providing your professional e-mail, as well as your business contact information, when applicable.</p> <p>Our products and subscriptions are aimed at professionals, businesses, and non-for-profit organizations. A professional e-mail address is required to subscribe or receive newsletters.</p> <p>You can unsubscribe from receiving our newsletters at any time using the unsubscribe link in our communications, or by writing to us at privacy@henriwolf.law.</p>
<p>To process your payment for our products and services available through our website, including related regulatory and fraud monitoring processing.</p>	<p>We offer paid subscriptions and services through our websites, in which case, we are the merchant, and we use Stripe Checkout to process your payment. The session provides a URL that redirects to a Stripe-hosted payment page in which you can enter payment details and complete the transaction. After the session, a webhook fulfils the order. Henri & Wolf does not store nor access your credit card information.</p> <p>Stripe also conducts fraud monitoring and prevention. For instance, their address verification services (AVS) verifies that the postal code and billing address corresponds with the information in the credit card issuer's records and ensure that the card verification code (CVC) behind the card matches with the information on record. When this information does not match, transactions can be automatically rejected. You can use other payment methods by contacting us at contact@henriwolf.law.</p> <p>You can read Stripe's privacy notice at https://stripe.com/en-ca/privacy. Stripe complies with strict security requirements under the norm PCI DSS. Click here to learn more about our security practices.</p> <p>To conduct a transaction, we collect transaction data that may include the following: your name, email address, billing address, shipping address, payment method information (such as credit or debit card number, bank account information or payment card image</p>

	<p>selected by you), merchant and location, purchase amount, date of purchase, phone number. We also collect information about your purchase, such as the type of service or product selected.</p>
<p>To process your request to join our community or to get more information on our community.</p>	<p>If you want to join our community or obtain more information, you can reach out to us through our website, including to submit your resume. We do not use your personal data submitted for this purpose for other purposes.</p> <p>The personal data that we process for this purpose includes any information on your resume, your certifications, professional memberships, and references. We will verify your reference and review your certifications and attestations.</p> <p>A criminal background check is mandatory due to the nature of the data that we process as part of our services, and due to our clients' requirements. We do not automatically reject applications if there is a criminal infraction, but for us to review your application further, you will be required to disclose additional information for our considerations.</p>
<p>To respond to your inquiries, including when you complete a form on our website.</p>	<p>You can reach out to us with questions, inquiries, and requests. Naturally, we need to process this information to respond to it. Business contact information for inquiries is managed through HubSpot and we apply reasonable retention periods.</p> <p>You can also decide to share personal data with us when you download content, such as a white paper, comment on our content, or otherwise register to our events.</p>
<p>To conduct digital advertising, including retargeting based on business contact information.</p>	<p>We use LinkedIn and Google to provide advertising and conduct retargeting. We only conduct retargeting based on business contact information and professional interests. We're not interested in your private life, nor in the types of cookies that you eat on weekend, but you can click here to learn more about the cookies that we use on our website and click here to learn more about our digital advertising practices.</p> <p>We use HubSpot, a customer relationship management tool, to manage our business contacts, and segment them based on industries, or similar commercial segmentation. Here again, we don't profile individuals based on their personal life. Our clientele is corporate, and we organize our activities accordingly. For instance, when you complete forms and share your business contact information, it will create an entry into HubSpot. We apply retention periods to our activities, click here for more details.</p>
<p>To ensure the security of our website.</p>	<p>Ensuring the security of the website and other online services requires processing personal data such as your IP addresses, and some data about browsing behavior on the site, such as the time of certain transactions. This data helps us detect and prevent security threats such as hacking attempts or malicious software.</p>

	For instance, we use a Web Application Firewall (“WAF”) that monitors and filters incoming traffic to our website. A WAF requires the processing of IP addresses, HTTP headers containing information about your browser and operating system being used by visitors, URL, post data and query strings. These can present signs of malicious patterns or activities, such as SQL injection attacks.
To analyse the performance of our website and obtain analytical data	We use cookies to analyse the performance of our website and obtain analytical data. We use Google Analytics to track website performance and obtain data such as page views, time on page, and bounce rate. We also use cookies to track the performance of our website in terms of traffic and use. This helps us understand better how our website is performing and obtain analytics on traffic and use. We do not share this data with third parties. We also use cookies to store information about your preferences and settings, such as language preferences. Keep reading to find out about our use of cookies for performance and analytics purpose.

3. What types of cookies do we use?

Cookies are used on our website. Cookies are text files which are downloaded on your browser to collect data within this browser, such as when you are navigating from one website to another one. Cookies can be installed by a website owner, or by third parties who are authorized to do so by the website owner. These third-party cookies generally include analytics and targeting cookies, which require remembering a past behavior when using the browser. We use both types of cookies through our website.

Third-party cookies collect data about you through several websites, and only make aggregated and traffic data available to us. We are unable to identify you specifically or build profiles about you. However, the third-party that we allow to install the cookies has access to this data. We offer you the opportunity to control which types of cookies can be installed when you navigate our website. If you do not want any third-party cookies to be able to retain data about your usage of the browser, you can disable analytic and targeting cookies.

First party cookies generally involve essential and functional cookies that help improve your use of the website. If you are looking to reduce your digital footprint without affecting your experience, turning off third-party cookies can help. There are also options to prevent specific third parties from installing cookies on your browser. [Click here](#) to know how to manage your preferences regarding cookies.

Please note that we do not currently respond to “Do Not Track Signals”.

[Click here to learn about the types of cookies that we use.](#)

Cookies are generally classified in the categories described below. Through our website, you can decide which categories of cookies you allow us to install. You can also learn about more specific options by [clicking here](#). In the table below, you can find an overview of each category of cookies, with examples.

Types of cookies	Explanations
Essential	<p>Essential cookies, also referred to as “strictly necessary”, are essential for the proper functioning of a website. These cookies are used to handle user input, support security measures, and facilitate network communication. They help users navigate the website, such as by keeping them logged in. Our website utilizes essential cookies.</p> <p>Examples include __cfuid and __cf_bm which are associated with sites utilizing CloudFlare, to identify trusted web traffic and differentiate between humans and bots respectively.</p>
Functional	<p>Functional cookies are used to remember choices you may have made, such as language preferences, or to remember your settings for a service. They are also used to provide certain services or features you have requested, such as watching a video or commenting on a blog. Our website uses functional cookies, such as for consent management. The personal data collected for this purpose includes IP addresses, device information and browser types.</p>
Analytical	<p>Analytical cookies are used on our website to gain insight into how visitors interact with it. These cookies track which pages are most visited and help to optimize the user experience. This data is used to measure the effectiveness of our marketing strategies, reduce the repetition of advertisements, and customize content to make our website more intuitive and user-friendly. The collected data includes traffic data, conversion data, user preferences, pages visited, the source website, downloaded content, and search terms used to navigate the site. This aggregate analytic data helps us improve the user experience and the quality of our website, products and services, or the effectiveness of our advertising practices.</p>
Marketing	<p>These are cookies to tailor ads to your interests based on your online activities, e.g., if you browsed websites relating to technology law. These cookies can remember that a device has been on a site or a service and may track activity on other sites too.</p> <p>For instance, LinkedIn marketing cookies provide insights about LinkedIn members who engage with our online services. They help deliver targeted ads on LinkedIn based on your interests. Click here to learn more about our digital practices.</p>

[Click here to find out how you can verify independently which cookies are on a website.](#)

If you want to find out what cookies are used by your favorite websites, there are several free cookie scanners that you can use to verify and analyze them. These cookie scanners allow you to identify and check the types of cookies, their duration and purpose, and other relevant information. With this information, you can make sure that the cookies are used responsibly and securely.

[Click here to learn about our use of the Google products.](#)

We use Google Analytics as part of our online activities. Google Analytics is a web analytics service offered by Google that tracks and reports website traffic to provide us with insights. Here's how data processing through Google Analytics work:

1. **Data Collection:** Our site uses Google Analytics to gather data about your visit. This includes which pages you view, what you click on, your device type, location, and how you found our site. This information is collected through cookies and JavaScript code embedded in our site.
2. **Data Processing:** Google Analytics turns the collected data into readable reports. It combines data from different visits and organizes it by factors such as location, device, or visit time.
3. **Data Configuration:** The data is then arranged to fit our analysis needs. This can involve creating custom reports, defining goals, and filtering out unnecessary data.
4. **Data Reporting:** The processed data is made available in various Google Analytics reports. These reports give us insights like the number of visitors, the pages they visited, their stay duration, and other performance indicators.

We can't track you individually; we only receive traffic data.

You can control which cookies Google can install on your browser. [Click here](#) for more information.

4. How do we use digital advertising, and do we conduct interest-based advertising?

We do conduct interest-based advertising; however, it is limited to professional interests. We do not target any personal characteristics of individuals, such as their gender, age, or favorite sports. We use platforms such as LinkedIn for targeting audiences, and Google for retargeting when you search for relevant topics such as "cybersecurity lawyers". Keep reading to the next question to understand how you can manage your preferences: you will find a detailed guides. You are in control.

[Click here for more info.](#)

LinkedIn's pixel, also known as the LinkedIn Insight Tag, is a piece of lightweight JavaScript code that you can add to your website to enable campaign reporting and unlock valuable insights about your website visitors.

When a LinkedIn member visits your website, the pixel is activated, and an anonymous cookie is set in their browser. This cookie collects metadata such as the URL, IP address, device and browser characteristics, and timestamp. This data is encrypted, then de-identified within seven days, and the de-identified data is deleted within 90 days.

LinkedIn does not share the personal data collected with its advertising customers. Instead, it provides them with aggregated reports about the website audience and ad performance.

Interest-based advertising is a way of serving ads that are likely to be more relevant to the user, based on information about their interests. These interests are inferred from data collected about the user's browsing behavior, either on a single website or across multiple sites.

On LinkedIn, interest-based advertising may involve serving ads to users who have shown an interest in a particular industry, job function, or company, based on their activity on LinkedIn. LinkedIn's interest-based advertising respects user privacy and adheres to privacy laws and regulations. Users can control their ad settings and opt out of interest-based advertising at any time.

AdRoll is a marketing platform that provides automation, insights, and personalization to help businesses reach their growth goals. It offers a suite of tools for online advertising, email marketing, and on-site engagement to help businesses attract, convert, and grow their customer base. AdRoll uses artificial intelligence and machine learning to automate marketing tasks, analyze data, and personalize content and ads to individual customers.

5. How can you manage your preferences regarding cookies and digital advertising?

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](#)

You can install the Google Analytics opt-out browser add-on, which prevents the Google Analytics JavaScript (ga.js, analytics.js and dc.js) from sharing information with Google Analytics about visits activity. For more information on the privacy practices of Google, please visit the [Google Privacy & Terms](#).

To know more about why you are seeing an ad, how to control and/or opt-out of marketing cookies and tracking technologies for interest-based advertising, please visit the [Digital Advertising Alliance of Canada website](#) for more information on the AdChoices Tools. You can also consult [Google Ads](#).

6. With whom do we share your personal data, and why?

The principle is that we only share your personal data with our service providers. There are a few exceptions that may apply, such as if we must comply with a legal request. Of course, if you comment on our content, or otherwise on our social media, this information will be publicly available to third parties, such as other individuals navigating the website or interacting with us on social media. We can also disclose personal data as part of a commercial transaction, but always subject to our ethical duties as a law firm, and the laws that apply to us, and our profession. In any case, this statement will continue to apply in case of a change of ownership, or in case we sell part or all our assets.

[Click here for more information.](#)

Below is a more detailed list of the categories of third parties with whom we share your personal data, along with specific examples. You can reach out to our Privacy Officer at privacy@henriwolf.law for an updated and complete list at any time.

Categories	Explanations
Service Providers	
Information Technology	As with any other website, we use IT service providers to host it and make it available to you. Our website is hosted by OVH. We also use WordPress as a backend for our website. You may access OVH's privacy policy and terms and conditions here: https://www.ovhcloud.com/en-ca/terms-and-conditions/contracts/
Customer Management	n/a
Communications	n/a
Payment Provider	We use Stripe to process your payments for our products and services. We only use Stripe Checkout, and as such, your credit card payment information is hosted entirely by Stripe, in their environment, not in ours. You can consult Stripe's privacy notices by here: https://stripe.com/en-ca/privacy .
Third Parties	
Marketing Partners	Although we do not sell any personal data, we do authorize some third parties, such as LinkedIn, to install pixels on our website. These pixels can collect personal data about you. Click here to learn more about our advertising practices and click here to learn how to manage your preferences regarding cookies.
Affiliates	As we continue to expand our activities, we may share personal data between our affiliates, but only as necessary to conduct our digital activities efficiently, and subject to an intra-company agreement.
Law Enforcement and Regulatory Authorities	If we are required by law to share your personal data with the authorities, including law enforcement or as part of an enforcement actions by data protection authorities, or because of a court order, we ensure that we follow a procedure that minimally involves: <ul style="list-style-type: none"> - Validating that the request is justified and proportional. - Assessing whether we should take actions to minimize or contest the disclosure request. - Informing the concerned individuals, when appropriate. - Disclosing only the information minimally required to comply with the requirements, and to the extent possible, ensuring that the disclosure is subject to appropriate security measures.

7. How do we protect your personal data?

As a community, we also have our own security controls that include:

- Leveraging threat intelligence and dark net monitoring to ensure that our members' identity have not been leaked or their credentials compromised. We also monitor our domains.
- Maintaining a Microsoft security score above industry average and enabling single sign on (SSO) authentication whenever possible.
- Multifactor authentication (MFA) is mandatory: our members also receive their own YubiKey when joining the community. We enforce access on a need-to-know basis and actively engage with our providers to understand their security roadmap. When members leave us for other horizons, their accesses are immediately revoked.
- All new members joining the community receive a walk-through regarding their security configurations on their devices.
- Our members receive regular updates on vulnerabilities that can affect their devices, both professionals and personals. Several awareness communications are sent through the community chat, including on risks specific to the legal industry.
- All members of the community have executed a detailed agreement that covers security, privacy, and confidentiality obligations. Verifications regarding criminal files are in the process of being completed for all our permanent members.
- We maintain written policies and procedures that are proportional for our needs, including for data retention, as well as consequent insurance coverage.

You can consult our Trust Center by [clicking here](#). We are constantly working on improving, including by publishing our policies and practices.

About payment security.

Stripe Checkout is a secure and PCI DSS compliant payment processor that uses HTTPS and AES-256 encryption to protect sensitive data. All card numbers are encrypted, and the decryption keys are stored on separate machines. Stripe is a PCI Service Provider Level 1 and is regularly audited to ensure the highest security standards.

About our service providers.

We strive to use services that provide transparency about their data security and privacy controls, and which are audited by independent services.

Our cloud service provider maintains several certifications and certifications, which means that it is audited by independent third parties. These include industry standards such as CSA Star and ISO/IEC 27001. Detection systems are integrated in the global monitoring system of OVH's data centers, and a dedicated security team is present in each data center. The French National Cybersecurity Agency (ANSSI) certified OVH's private cloud offering as fulfilling the highest standards of security in Europe. You can consult OVH's Trust Center here: <https://corporate.ovhcloud.com/en/trusted-cloud/security-certifications/>.

For instance, you can consult HubSpot's Trust Center by [clicking here](#). This allows you to download their SOC3 and SOC 2 Type 2 reports, latest penetration test summaries, and security overview. HubSpot's uses a defense-in-depth approach to implement layers of security that leverages compliance and regulatory requirements, but also industry best practices like the OWASP Top 10 and CIS Critical Security Controls.

8. Where do we store your personal data?

Our website is hosted in Quebec, Canada. However, as part of our digital activities, we use service providers that are in other countries. For instance, HubSpot is used for customer relationship management, and is hosted in the United States. Stripe Checkout is also hosted in the United States and will have access to the payment information that you enter when purchasing goods and services. We do not have access to this information from Canada. You always have the option to reach out to us at contact@henriwolf.law if you do not want to share your payment information with a company outside of Canada.

We have contracts with our service providers, and we perform due diligence based on the risks related to the processing of your personal data. We prioritize suppliers that are audited by independent third parties regarding their security and privacy practices.

Nonetheless, when your personal data is transferred outside of the jurisdiction in which you are located, different laws may be applicable to such personal data. This may allow foreign government to access your personal data, under certain legal frameworks. If you have any concerns with the sharing of your personal data in the United States, our Privacy Officer can respond to your concerns and work with you to limit international transfers through work arounds: privacy@henriwolf.law.

9. How long do we retain your personal data?

When we collect your personal data, we make sure that we have a purpose, and that our retention is aligned with this purpose. Once this purpose is achieved, we delete it, unless the law requires keeping it for longer. We have adopted a [Data Retention Policy](#), which is available in our [Trust Center](#). We also maintain a data retention schedule, which identifies the retention periods for each type of data, along with the way it should be securely deleted. When our Chief Technology Officer sets up our IT systems, he ensures that configurations are in place to automate the deletion of your personal data safely. You can reach out to our Privacy Officer to get a better understanding of how we

10. What are your personal data rights, and how can you exercise them?

Depending on where you are located and applicable laws, you benefit from different rights over your personal data. These rights generally include the right to access your personal data, to withdraw your consent, or to modify your personal data when it is inaccurate.

Contact our Privacy Officer by e-mail at privacy@henriwolf.law to exercise your rights, or by mail at the following address:

[Henri & Wolf, Inc.](#)

At the attention of: Privacy Officer
731 De la Commune St W, Bureau 100
Montreal, Quebec
H3C 1X7, Canada

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.

Version 0.1

We may need to collect additional personal data to confirm your identity and respond to your request. We will not use this personal data for other purposes.

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 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](#). In Quebec, you can also contact the [Commission d'accès à l'information](#). If you are in the EU, you can find the list of data protection authorities [here](#).

11. Can we update this Website Privacy Statement?

Absolutely, it is necessary for many reasons such as complying with new legal requirements and reflecting new processing of personal data, or changes to existing ones. We are in full expansion, and we have a lot of plans. We want to make sure that we remain transparent with you. You can see the latest date at which we updated this statement at the top of the page, and we make all previous versions available to you for consultation. If you are registered to one of our newsletters, we will notify you of any material changes that you should know about. Otherwise, we encourage you to have a look at our Trust Center from time to time to know what has changed!

* * *