

INSECUREWEB, LLC PRIVACY POLICY

This privacy policy (“**Privacy Policy**”) sets out the basis on which **InsecureWeb, LLC** (hereinafter referred to as “**Company**”, “**we**”, “**our**” or “**us**”, may collect, process, use and disclose Personal Data (defined below):

- about each client, individual, entity, user, or visitor (collectively “**you**” or “**your**”);

and/or

- which you provide to Company when accessing Company’s web-based software-as-a-service (SaaS) digital attack surface analysis platform, and/or website located at insecureweb.com (collectively the “**SaaS Platform**”) and when using the dark web monitoring services/solutions provided by Company to its clients via the SaaS Platform (the “**Dark Web Monitoring Service(s)**”).

Company is committed to protecting your privacy and the confidentiality of your Personal Data (defined below). As such, our Privacy Policy is designed to help you understand how we collect, store, use and safeguard the information you provide to us and to assist you in making informed decisions when using the Dark Web Monitoring Services.

By accessing the SaaS Platform and using the Dark Web Monitoring Services, you accept the terms and conditions of Company’s Privacy Policy, and you consent to Company’s collection, storage, use and disclosure of your Personal Data (defined below) as described in this Privacy Policy.

We encourage you to read this Privacy Policy carefully so that you know and understand the purposes for which Company collects, processes, uses and shares your Personal Data.

1. Definition of Personal Data and Non-Personal Data

The term “**Personal Data**” shall refer to data about an individual which can be used to identify the individual either (i) from that data, or (ii) from that data in combination with other information to which Company may have access to or is likely to have access.

“**Non-Personal Data**” includes information that cannot be used to personally identify you, such as general demographic information we may collect, referring/exit pages and URLs, platform types, device types, preferences you submit and preferences that are generated based on the data you submit.

2. Scope of Privacy Policy

This Privacy Policy governs your access of Company’s SaaS Platform and Dark Web Monitoring Services, regardless of how you access the SaaS Platform and Dark Web Monitoring Services, and explains what data we collect when you use the SaaS Platform and/or Dark Web Monitoring Services, why we collect the data, how data is used, and your rights and choices. This Privacy Policy applies to Personal Data and Non-Personal Data collected by us from or about our clients, visitors to, or users of, our SaaS Platform.

Although we take reasonable precautionary steps, we do not control how a third party service provider may use your Personal Data. Please note that third party service providers may have their own privacy policies and we are not responsible for the third party service providers actions, including their handling of Personal Data. As such, please review the privacy policies

of each third party service provider for more information on how they use the personal data they collect.

3. Dark Web Monitoring Services

Company collects and stores both the Personal Data that you provide to us and the Personal Data that is publicly available from the dark web so as to ascertain whether your Personal Data has been exposed, stolen or compromised.

Company collects, stores and processes information from the dark web:

- (i) by taking the necessary precautions, including the use of an encrypted connection and virtual private network;
- (ii) using legitimate credentials as provided by the dark web forums operators;
- (iii) solely for the purposes of providing the Dark Web Monitoring Services to its clients;
- (iv) for legitimate cybersecurity purposes (e.g., to help clients identify and defend against cybersecurity threats); and
- (v) with no criminal, fraudulent or malicious intent or motive.

4. Personal Data Company Collects from You

Company may collect, store, process, use, and disclose the following Personal and Non-Personal Data obtained from you:

- (i) **Identity data** includes your first name and surname;
- (ii) **Contact data** which includes data such as billing address, email address and phone number, and any other data you have provided to us in order for us to be able to provide you with the Dark Web Monitoring Services on the SaaS Platform;
- (iii) **Financial data** such as your payment card details;
- (iv) **Transaction data** which includes details about payments and communications to and from you;
- (v) **Technical data** which includes your Internet protocol address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the SaaS Platform;
- (vi) **Usage data** includes information about your visits to and use of our SaaS Platform and Dark Web Monitoring Services; and
- (vii) **Marketing data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

In the context of the law and this Privacy Policy, the term “*process*” means collect, store, transfer, use or otherwise act on information.

5. Use of your Personal Data

Personal Data submitted via the SaaS Platform will be used for the purposes specified in this Privacy Policy. As such, Company may collect, store and use your Personal Data for any or all of the following purposes:

- (i) providing you with the Dark Web Monitoring Services;
- (ii) verifying your identity;
- (iii) providing you with access to the SaaS Platform;
- (iv) responding to, handling, and processing queries, requests, complaints, and feedback from you;
- (v) managing your relationship with us;

- (vi) processing payment or credit transactions;
- (vii) sending you information, promotions, updates, and marketing and advertising materials in relation to our Dark Web Monitoring Services;
- (viii) managing, developing and improving our business and operations to serve you better;
- (ix) complying with legal and regulatory requirements;
- (x) enforcing Company's legal rights and obligations;
- (xi) any other purposes for which we have obtained your consent; and
- (xii) any other purposes reasonably necessary, ancillary or related to the above specified purposes.

Except as otherwise stated in this Privacy Policy, Company does not sell, trade, rent or otherwise share your Personal Data with third parties without your consent.

Company may share Personal Data with out third party service providers if Company has a good-faith belief that access, use, preservation or disclosure of the Personal Data is reasonably necessary to meet any applicable legal process or enforceable governmental request; to enforce the terms and conditions of Company's Dark Web Monitoring and Digital Attack Surface Analysis Software-as-a-Service Master Services Agreement, including investigation of potential violations; detection and prevention of misuse of the Dark Web Monitoring Services, address fraud, security or technical concerns; or to protect against harm to the rights, property or safety of Company's users or the public as required or permitted by law.

Wherever possible, Company aims to obtain your explicit consent to process your Personal Data. We may continue to process your Personal Data on this basis until you withdraw your consent. You may withdraw your consent at any time by sending us an email at enterprise@insecureweb.com. However, if you do so, please note that you may not be able to use the SaaS Platform and make use of the Dark Web Monitoring Services further.

6. Use of Non-Personal Data

Company may collect information about your computer and visits to the SaaS Platform for administration purposes and to improve the SaaS Platform's usability. All Non-Personal Data is anonymous and cannot be used to identify any user of the SaaS Platform.

Company shares only Non-Personal Data with vendors and suppliers who are performing services for Company, such as the vendors and suppliers who provide Company with access to a user's email address and email communications for the purposes of Company being able to send emails to you via the vendor and/or supplier's server. Those vendors and suppliers use your Non- Personal Data only at Company's direction and in accordance with our Privacy Policy.

Generally, Company uses Non-Personal Data to help us improve the Dark Web Monitoring Services and customize your user experience. We also aggregate Non-Personal Data in order to track trends and analyze use patterns on the SaaS Platform. This Privacy Policy does not limit in any way our use or disclosure of Non-Personal Data and we reserve the right to use and disclose such Non-Personal Data to our partners, advertisers and other third parties in Company's sole discretion.

7. Automatic Collection of Information

When you visit the SaaS Platform, Company's servers automatically record information about your computer hardware and software (such as domain names and IP addresses). No Personal Data is collected or revealed by this process. The information is collected automatically and is used only to identify potential cases of abuse, resolve technical issues,

optimize the performance of the SaaS Platform for a better user experience, and establish statistical information regarding your use of the SaaS Platform and Dark Web Monitoring Services. This statistical information is not otherwise aggregated in such a way that would identify any particular user of the system.

8. How Personal Data is Secured

Company will take appropriate technical, organizational and information security safeguards to prevent the loss, misuse or alteration of your Personal Data. These safeguards include firewalls, virtual networks, network segmentation, web application firewall, SIEM system, incident response, bi-annual penetration testing, physical and digital security measures, encryption, access restrictions, password authorization, system logging, and file backup. Company only has access to encrypted Personal Data as required to fulfill the Dark Web Monitoring Services.

Company's database servers shall be hosted and secured by OVHcloud (<https://www.ovhcloud.com/en/enterprise/certification-conformity/>).

Of course, data transmission over the Internet is inherently insecure, and as such you acknowledge that no data transmission over the Internet or wireless network can be guaranteed. Therefore, while Company strives to protect your Personal Data, you acknowledge that (i) there are security and privacy limitations of the Internet which are beyond our control; (ii) the security, integrity, and privacy of any and all information and data exchanged between you and another user or Company on the SaaS Platform and/or the Dark Web Monitoring Services cannot be guaranteed; and (iii) any such information and data may be viewed or tampered with in transit by a third-party, despite Company's best efforts.

9. Your Rights under the General Data Protection Regulation

For the purposes of complying with the General Data Protection Regulation 2016/679 ("GDPR"), Company is considered as the data controller in relation to your Personal Data. We have listed below, the principal rights you have under the GDPR:

- (i) the right to access - you can ask for copies of your Personal Data;
- (ii) the right to rectification - you can ask us to rectify inaccurate Personal Data and to complete incomplete Personal Data;
- (iii) the right to erasure - you can ask us to erase your Personal Data from our systems;
- (iv) the right to restrict processing - you can ask us to restrict the processing of your Personal Data;
- (v) the right to object to processing - you can object to the processing of your Personal Data;
- (vi) the right to data portability - you can ask us to transfer your Personal Data to another organization or to you;
- (vii) the right to complain to a supervisory authority - you can complain about our processing of your Personal Data to the applicable authorities; and
- (viii) the right to withdraw consent – you can request that we withdraw your consent to store and process your Personal Data except to the extent that the basis of our processing your Personal Data is required by law.

You may exercise any of your rights in relation to your Personal Data by written notice to Company, using the contact details set out below. Should you have any cause for complaint about our use of your Personal Data, please contact Company using the details provided below and we will endeavor to solve the problem for you.

10. Your Rights under the California Consumer Privacy Act

To the extent that the California Consumer Privacy Act (“**CCPA**”) is applicable to either Company or you: both parties agree to comply with all of its obligations under the CCPA; and in relation to any communication of ‘*personal information*’ as defined by the CCPA, the parties agree that no monetary or other valuable consideration is being provided for such personal information and therefore neither party is ‘*selling*’ (as defined by the CCPA) personal information to the other party.

The principal rights you have under the CCPA include but are not limited to:

- (i) the right to know the Personal Data we collect from you;
- (ii) the right to request the deletion of your Personal Data;
- (iii) the right not to be discriminated against for having exercised your rights under the CCPA;
- (iv) the right to opt out from the collection/sale of your Personal Data; and
- (v) the right to access your Personal Data.

Both parties agree to notify the other immediately if it receives any complaint, notice, or communication that directly or indirectly relates to either party’s compliance with the CCPA. Specifically, Company shall notify you within ten (10) business days if Company receives a verifiable consumer request under the CCPA.

11. Analytical Data from Third Parties

Company may collect or receive information that third party service providers may provide about you when using the SaaS Platform and/or the Dark Web Monitoring Services. Or Company may obtain information from other sources and combine that with information Company collects through your use of the Dark Web Monitoring Services. The following information is collected and/or obtained from third parties:

- (i) **Google Analytics:** We use this analytical tool to help Company analyze (i) how users use the SaaS Platform and/or the Dark Web Monitoring Services by noting when you use the SaaS Platform and the Dark Web Monitoring Services, and (ii) usage data and performance data. The information collected will be disclosed to or collected directly by the applicable analytical tool Company is using. Such information is collected as a means to provide, improve, and develop the SaaS Platform and the Dark Web Monitoring Services so as to create a safer and trusted environment when you use the SaaS Platform and the Dark Web Monitoring Services.
- (ii) **Zoominfo:** We use this analytical tool to measure the effectiveness of our advertising campaigns by understanding your interests so that we may use this information to improve and develop our SaaS Platform and the Dark Web Monitoring Services.
- (iii) **Salesloft:** We use this tool to understand and gain insight on how you use the SaaS Platform, to identify and test your usage of the SaaS Platform’s functions, and to further analyze usage data, performance data, to statistically analyze user behavior and activity, and to obtain feedback from you on your usage of the SaaS Platform and Dark Web Monitoring Services we provide.

Analytical data received from third parties is only used for Company’s internal marketing purposes and is shared with Company’s subsidiaries or parent company, and is not sold to any third party.

12. Cookies

Cookies are defined as small text files that are placed on your computer's hard drive by your web browser when you visit any website. Cookies allow data gathered on one web page to be stored until it is needed for use on another, allowing a website to provide you with a personalised experience and the website owner with statistics about how you use the website so that it can be improved. Some cookies may last for a defined period of time, such as one day or until you close your browser. Others last indefinitely. Your web browser should allow you to delete any you choose. It also should allow you to prevent or limit their use.

Company may from time-to-time use cookies. They are placed by software operated by third parties whose services Company makes use of so as to enhance your experience on the SaaS Platform.

When you first visit the SaaS Platform, you may need to confirm whether you wish for cookies to be used by Company. If you choose not to accept them, Company shall not use them for your visit except to record that you have not consented to their use for any other purpose. However, please note that should you choose not to use cookies, or you prevent their use through your browser settings, you might not be able to use all the functionalities available on the SaaS Platform.

Company may use cookies for the following purposes:

- (i) Authentication and status - Company uses cookies to identify you when you visit the SaaS Platform, and as you navigate through the pages of the SaaS Platform;
- (ii) Personalization - Company uses cookies to store information about your preferences as you navigate through the SaaS Platform;
- (iii) Security - Company uses cookies as an element of the security measures used to protect the SaaS Platform and Dark Web Monitoring Services; and
- (iv) Analysis - Company uses cookies to analyze the use and performance of the SaaS Platform and Dark Web Monitoring Services.

By accessing and using Company's SaaS Platform and Dark Web Monitoring Services, you consent to the storage of cookies, other local storage technologies, beacons and other information on your devices. You also consent to the access of such cookies, local storage technologies, beacons and information by us or our representatives or agents.

13. Retention Period for Personal Data

Except as otherwise mentioned in this Privacy Policy, Company shall endeavour to keep your Personal Data on file for up to ten (10) years (i) for Company to be able to provide you with the Dark Web Monitoring Services, (ii) to comply with the law, including for the period demanded by our tax authorities, or fraud prevention, and (iii) to support a claim or defence in court.

Company will permanently destroy your Personal Data on or before the ten (10) year anniversary of your use of the Dark Web Monitoring Services. After your Personal Data is destroyed, you will need to re-register (and provide your Personal Data to Company again) before you can use the Dark Web Monitoring Services.

14. Withdrawing Your Consent / Opt-out rights

Wherever possible, Company aims to obtain your explicit consent to process your Personal Data. The consent that you provide to Company for the collection, use, storage, and disclosure of your Personal Data will remain valid until such time as you withdraw your consent in writing. You may withdraw your consent and request us to stop using and/or disclosing your Personal Data for any or all of the purposes by:

- (i) submitting your request via email enterprise@insecureweb.com, or
- (ii) removing the SaaS Platform from your mobile /computer device.

Upon receipt of your written request to withdraw your consent, you acknowledge that (i) Company may not be able to provide or continue providing you with access to the SaaS Platform and use of the Dark Web Monitoring Services, and (ii) we may cease such provision of the Dark Web Monitoring Services to you accordingly without any liability.

You acknowledge and understand that by withdrawing your consent, this does not affect our right to continue to collect, use and disclose Personal Data where such collection, use and disclose without consent is permitted or required under applicable laws.

15. Use of SaaS Platform and Dark Web Monitoring Services by Children

Our SaaS Platform and Dark Web Monitoring Services are not directed to persons under the age of eighteen (18) years. We do not collect Personal Data from children under the age of eighteen (18) years. We therefore encourage you to obtain the assistance and consent of a parent/legal guardian when accessing our SaaS Platform and using the Dark Web Monitoring Services. A parent/legal guardian who becomes aware that his or her child has provided us with Personal Data without their consent, should contact us at enterprise@insecureweb.com and we will endeavour to delete it.

16. Changes and Amendments to Privacy Policy

Company may update this Privacy Policy from time to time in Company's sole discretion and will notify you of any material changes to the way in which Company treats Personal Data. When changes are made, Company will revise the updated date at the bottom of this page. Company may also provide notice to you in other ways in Company's sole discretion, such as through the contact information you have provided. Any updated version of this Privacy Policy will be effective immediately upon the posting of the revised Privacy Policy unless otherwise specified. Your continued use of the SaaS Platform and Dark Web Monitoring Services after the effective date of the revised Privacy Policy will constitute your consent to those changes. However, Company will not, without your consent, use your Personal Data in a manner materially different than what was stated at the time your Personal Data was collected.

17. Contact Information

Should you have any questions or concerns regarding privacy while using the SaaS Platform and Dark Web Monitoring Services, please send us a detailed message to enterprise@insecureweb.com and Company will use its best endeavors to resolve your concerns.

Effective Date: 1st of June 2022.