
Privacy Policy

dnswatchdog.io



Welcome

We provide security tools for businesses of all sizes who use our technology and services to help audit their DNS portfolio to detect potential issues before they become incidents.

This Privacy Policy ("Policy") describes the Personal Data that we collect, how we use and share it, and how you can reach us with privacy-related inquiries. The Policy also outlines your rights and choices as a data subject, including the right to object to certain uses of your Personal Data.

Defined Terms

This Privacy Notice for DNS Watchdog Ltd. ('we', 'us', or 'our'), describes how and why we might access, collect, store, use, and/or share ('process') your personal information when you use our services ('Services'), including when you:

- Visit our website at <https://dnswatchdog.io> or any website of ours that links to this Privacy Notice.
- Use the DNS Watchdog application
- Engage with us in other related ways, including any marketing or events.

Summary of Key Points

This summary provides key points from our Privacy Notice, but you can find out more details about any of these topics by using the table of contents below to find the section you are looking for.

- **What personal information do we process?** When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and the products and features you use.
- **Do we process any sensitive personal information?** We do not process sensitive personal information.
- **Do we collect any information from third parties?** We do not collect any information from third parties.
- **How do we process your information?** We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so.
- **In what situations and with which parties do we share personal information?** We may share information in specific situations and with specific third parties.

- **How do we keep your information safe?** We protect your personal information with robust organisational and technical safeguards, including encryption in transit and at rest, strict access controls, and regular security reviews. While no system connected to the internet can eliminate all risk, we are committed to continuously strengthening our defences and responding swiftly to any emerging threats.
- **What are your rights?** Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information.
- **How do you exercise your rights?** The easiest way to exercise your rights is by submitting a data subject access request, or by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Table of Contents

1. What Information Do We Collect?
2. How Do We Process Your Information?
3. What Legal Bases Do We Rely On To Process Your Personal Information?
4. When And With Whom Do We Share Your Personal Information?
5. Do We Use Cookies And Other Tracking Technologies?
6. How Long Do We Keep Your Information?
7. How Do We Keep Your Information Safe?
8. Do We Collect Information From Minors?
9. What Are Your Privacy Rights?
10. Controls For Do-Not-Track Features
11. Do United States Residents Have Specific Privacy Rights?
12. Do We Make Updates To This Notice?
13. How Can You Contact Us About This Notice?
14. How Can You Review, Update, Or Delete The Data We Collect From You?

1. What Information Do We Collect?

Personal information you disclose to us

In Short: We collect personal information that you provide to us.

We collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Personal Information Provided by You. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you

make, and the products and features you use. The personal information we collect may include the following:

- Names
- Email addresses
- Contact preferences
- Billing addresses
- Contact or authentication data
- Usernames

Sensitive Information. We do not process sensitive information.

Payment Data. If you choose to make purchases, payment data (such as your payment card number and security code) is collected and processed directly by our payment processor, Stripe. We do not receive, access, or store your full payment card details. You may find Stripe's privacy notice here: <https://stripe.com/gb/privacy>.

All personal information that you provide to us must be materially true, complete, and accurate, and you must notify us of any material changes to such personal information.

Information automatically collected

In Short: Some information - such as your Internet Protocol (IP) address and/or browser and device characteristics - is collected automatically when you visit our Services.

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. You can find out more about this in our [Cookie Policy](#).

The information we collect includes:

- **Log and Usage Data.** Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called 'crash dumps'), and hardware settings).

- **Device Data.** We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information.

2. How Do We Process Your Information?

In Short: We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To provide and deliver the Services.** We process your information to synchronise and analyse DNS records from your DNS providers, perform security scans (port scanning, certificate monitoring, HTTP checks), capture and analyse website screenshots, and generate audit trails and change logs - all as part of the core service you have subscribed to.
- **To process payments and manage subscriptions.** We process your information to manage your subscription, process billing through Stripe, and maintain your service entitlements.
- **To communicate with you.** We may process your information to send you service-related notices, respond to your inquiries, and provide customer support.
- **To monitor and improve the Services.** We process your information for error monitoring, performance tracking, and internal analytics to maintain service reliability and improve the platform.
- **To comply with legal obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.

3. What Legal Bases Do We Rely On To Process Your Personal Information?

In Short: We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e. legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfil our contractual obligations, to protect your rights, or to fulfil our legitimate business interests.

If you are located in the EU or UK

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- **Contract Performance.** We process your information where it is necessary to perform the contract you have entered into with us - for example, to provide the DNS monitoring and security services you have subscribed to, to manage your account, and to process billing. This is our primary legal basis for most of the processing we carry out.
- **Legitimate Interests.** We may process your information where it is necessary for our legitimate business interests, provided those interests are not overridden by your rights. This includes error monitoring and logging to maintain service reliability, security scanning of customer-owned infrastructure, and maintaining audit trails for accountability. We carefully balance our interests against the impact on your privacy.
- **Consent.** We may process your information if you have given us permission (i.e. consent) to use your personal information for a specific purpose, such as analytics cookies. You can withdraw your consent at any time.
- **Legal Obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- **Vital Interests.** We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as situations involving potential threats to the safety of any person.

In legal terms, we are generally the 'data controller' under European data protection laws of the personal information described in this Privacy Notice, since we determine the means and/or purposes of the data processing we perform. This Privacy Notice does not apply to the personal information we process as a 'data processor' on behalf of our customers. In those situations, the customer that we provide services to and with whom we have entered into a data processing agreement is the 'data controller' responsible

for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.

If you are located in Canada

We may process your information if you have given us specific permission (i.e. express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e. implied consent). You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way
- For investigations and fraud detection and prevention
- For business transactions provided certain conditions are met
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim
- For identifying injured, ill, or deceased persons and communicating with next of kin
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced
- If the collection is solely for journalistic, artistic, or literary purposes
- If the information is publicly available and is specified by the regulations
- We may disclose de-identified information for approved research or statistics projects, subject to ethics oversight and confidentiality commitments

4. When And With Whom Do We Share Your Personal Information?

In Short: We may share information in specific situations described in this section and/or with the following third parties.

We may need to share your personal information in the following situations:

- **Service Providers.** We share your information with third-party service providers who perform services on our behalf, pursuant to written contracts that require them to protect your data. These include:

Provider	Purpose	Data Shared
AWS (Amazon Web Services)	Cloud infrastructure hosting	All platform data (hosted in EU, eu-west-2, London)
Clerk	Authentication and identity management	Names, email addresses, organisation membership, session data
Stripe	Payment processing and subscription billing	Subscription and billing data (Stripe processes payment card details directly; we do not access or store card numbers)
Sentry	Application error monitoring	Error traces and request metadata (may include user IDs and email addresses)
Vercel	Frontend hosting and content delivery	Application code and static assets (no customer personal data stored at rest)
Google Analytics	Website analytics	Anonymised usage data (only with your consent via the cookie banner)

For more details on our sub-processors, please see our [Data Processing Agreement](#).

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

5. Do We Use Cookies And Other Tracking Technologies?

In Short: We may use cookies and other tracking technologies to collect and store your information.

We may use cookies and similar tracking technologies (like web beacons and pixels) to gather information when you interact with our Services. Some online tracking technologies help us maintain the security of our Services and your account, prevent crashes, fix bugs, save your preferences, and assist with basic site functions.

We also permit third-party analytics services (specifically Google Analytics) to use tracking technologies on our Services to help us understand how visitors use the Site. We do not use marketing or advertising cookies, and we do not engage in targeted advertising or retargeting. Non-essential cookies are only set with your consent via our cookie banner.

Specific information about how we use such technologies and how you can refuse certain cookies is set out in our [Cookie Policy](#).

Google Analytics

We may share your information with Google Analytics to track and analyse the use of the Services. To opt out of being tracked by Google Analytics across the Services, visit <https://tools.google.com/dlpage/gaoptout>. For more information on the privacy practices of Google, please visit the Google Privacy & Terms page.

6. How Long Do We Keep Your Information?

In Short: We keep your information for as long as necessary to fulfil the purposes outlined in this Privacy Notice unless otherwise required by law.

We will only keep your personal information for as long as it is necessary for the purposes set out in this Privacy Notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements).

The following table summarises our key retention periods:

Data Type	Retention Period
Account information	Retained while your account is active; deleted upon account closure
DNS records (active)	Retained while the provider connection is active; deleted when the provider is removed

Data Type	Retention Period
Archived DNS records	Up to 3 years (available for restoration during this period)
Screenshots	365 days (transitioned through storage tiers before deletion)
Audit trail and change logs	Up to 3 years
Scan history	Up to 2 years
Application logs	Per CloudWatch log group retention settings
Error reports (Sentry)	Per Sentry's data retention configuration
Subscription and billing data	Retained per legal requirements (managed through Stripe)

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

7. How Do We Keep Your Information Safe?

In Short: We protect your personal information with robust organisational and technical safeguards and are committed to continuously improving our security posture.

We have implemented appropriate and reasonable technical and organisational security measures designed to protect the security of any personal information we process. These include encryption of data in transit and at rest, strict role-based access controls, regular security reviews, and infrastructure hardened in line with industry best practices. While no system connected to the internet can eliminate all risk, we are committed to continuously strengthening our defences, monitoring for threats, and responding swiftly to any security events. You should only access the Services within a secure environment.

8. Do We Collect Information From Minors?

In Short: We do not knowingly collect data from or market to children under 18 years of age.

We do not knowingly collect, solicit data from, or market to children under 18 years of age or the equivalent age as specified by law in your jurisdiction, nor do we knowingly

sell such personal information. By using the Services, you represent that you are at least 18 or the equivalent age as specified by law in your jurisdiction or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age or the equivalent age as specified by law in your jurisdiction has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18 or the equivalent age as specified by law in your jurisdiction, please contact us at dpo@dnswatchdog.io.

9. What Are Your Privacy Rights?

In Short: Depending on your state of residence in the US or in some regions, such as the EEA, UK, Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. If a decision that produces legal or similarly significant effects is made solely by automated means, we will inform you, explain the main factors, and offer a simple way to request human review. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us using the contact details provided in the section 'How Can You Contact Us About This Notice?' below.

We will consider and act upon any request in accordance with applicable data protection laws. Under GDPR, we will respond to your request without undue delay and in any event within one (1) calendar month of receipt. This period may be extended by a further two (2) months where necessary, taking into account the complexity and number of requests, in which case we will inform you of the extension within the first month.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your Member State data protection authority or UK data protection authority. In the UK, the relevant authority is the Information Commissioner's Office (ICO), which can be contacted at <https://ico.org.uk>.

If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner (FDPIC) at <https://www.edoeb.admin.ch>.

Withdrawing your consent

If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us using the contact details provided in the section 'How Can You Contact Us About This Notice?' below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications

You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, or by contacting us using the details provided in the section 'How Can You Contact Us About This Notice?' below. You will then be removed from the marketing lists. However, we may still communicate with you - for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. For further information, please see our [Cookie Policy](#).

If you have questions or comments about your privacy rights, you may email us at privacy@dnswatchdog.io.

10. Controls For Do-Not-Track Features

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ('DNT') feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognising and implementing DNT signals has been finalised. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Notice.

California law requires us to let you know how we respond to web browser DNT signals. Because there currently is not an industry or legal standard for recognising or honouring DNT signals, we do not respond to them at this time.

11. Do United States Residents Have Specific Privacy Rights?

In Short: If you are a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, or Virginia, you may have the right to request access to and receive details about the personal information we maintain about you and how we have processed it, correct inaccuracies, get a copy of, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law.

Categories of Personal Information We Collect

The table below shows the categories of personal information we have collected in the past twelve (12) months.

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	YES
B. Personal information (California Customer Records statute)	Name, contact information, education, employment, employment history, and financial information	NO
C. Protected classification characteristics	Gender, age, date of birth, race and ethnicity, national origin, marital status, and other demographic data	NO
D. Commercial information	Transaction information, purchase history, financial details, and payment information	NO
E. Biometric information	Fingerprints and voiceprints	NO
F. Internet or other similar network activity	Browsing history, search history, online behaviour, interest data, and interactions with our and other websites, applications, systems, and advertisements	NO
G. Geolocation data	Device location	NO
H. Audio, electronic, sensory, or similar information	Images and audio, video or call recordings created in connection with our business activities	NO

Category	Examples	Collected
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us	NO
J. Education Information	Student records and directory information	NO
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	NO
L. Sensitive personal Information		NO

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels
- Participation in customer surveys or contests
- Facilitation in the delivery of our Services and to respond to your inquiries

Sources of Personal Information

Learn more about the sources of personal information we collect in [What Information Do We Collect?](#)

How We Use and Share Personal Information

Learn more about how we use your personal information in the section [How Do We Process Your Information?](#)

Will your information be shared with anyone else?

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about how we disclose personal information in the section [When And With Whom Do We Share Your Personal Information?](#)

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be 'selling' of your personal information.

We have not disclosed, sold, or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. We will not sell or share personal information in the future belonging to website visitors, users, and other consumers.

Your Rights

You have rights under certain US state data protection laws. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law. These rights include:

- Right to know whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request the deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to non-discrimination for exercising your rights
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ('profiling')

Depending upon the state where you live, you may also have the following rights:

- Right to access the categories of personal data being processed (as permitted by applicable law, including Minnesota)
- Right to obtain a list of the categories of third parties to which we have disclosed personal data (as permitted by applicable law, including California, Delaware, and Maryland)
- Right to obtain a list of specific third parties to which we have disclosed personal data (as permitted by applicable law, including Minnesota and Oregon)
- Right to obtain a list of third parties to which we have sold personal data (as permitted by applicable law, including Connecticut)
- Right to review, understand, question, and correct how personal data has been profiled (as permitted by applicable law, including Connecticut and Minnesota)
- Right to limit use and disclosure of sensitive personal data (as permitted by applicable law, including California)

- Right to opt out of the collection of sensitive data and personal data collected through the operation of a voice or facial recognition feature (as permitted by applicable law, including Florida)

How to Exercise Your Rights

To exercise these rights, you can contact us by submitting a data subject access request, by emailing us at privacy@dnswatchdog.io, or by referring to the contact details at the bottom of this document. We will respond to verifiable requests within forty-five (45) days of receipt, as required by applicable US state privacy laws. We may extend this period by an additional forty-five (45) days where reasonably necessary, in which case we will inform you of the extension.

Under certain US state data protection laws, you can designate an authorised agent to make a request on your behalf. We may deny a request from an authorised agent that does not submit proof that they have been validly authorised to act on your behalf in accordance with applicable laws.

Request Verification

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. We will only use personal information provided in your request to verify your identity or authority to make the request. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes.

If you submit the request through an authorised agent, we may need to collect additional information to verify your identity before processing your request and the agent will need to provide a written and signed permission from you to submit such request on your behalf.

Appeals

Under certain US state data protection laws, if we decline to take action regarding your request, you may appeal our decision by emailing us at privacy@dnswatchdog.io. We will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may submit a complaint to your state attorney general.

California 'Shine The Light' Law

California Civil Code Section 1798.83, also known as the 'Shine The Light' law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact details provided in the section 'How Can You Contact Us About This Notice?'

12. Do We Make Updates To This Notice?

In Short: Yes, we will update this notice as necessary to stay compliant with relevant laws.

We may update this Privacy Notice from time to time. The updated version will be indicated by an updated 'Revised' date at the top of this Privacy Notice. If we make material changes to this Privacy Notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

13. How Can You Contact Us About This Notice?

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO) by email at dpo@dnswatchdog.io, or contact us by post at:

DNS Watchdog Ltd. Data Protection Officer 167-169 Great Portland Street 5th Floor
London W1W 5PF United Kingdom

If you are a resident in the United Kingdom, we are the 'data controller' of your personal information. We have appointed Neil Saunders to be our representative in the UK. You can contact them directly regarding our processing of your information, by email at neil@dnswatchdog.io, or by post to:

DNS Watchdog Ltd. 167-169 Great Portland Street London W1W 5PF England

14. How Can You Review, Update, Or Delete The Data We Collect From You?

Based on the applicable laws of your country or state of residence in the US, you may have the right to request access to the personal information we collect from you, details about how we have processed it, correct inaccuracies, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. To request to review, update, or delete your personal information, please fill out and submit a data subject access request.