

Privacy Policy

Last updated: 5/5/2026

Sniffies, LLC (“**Sniffies**,” “**Company**,” or “**We**”) respect your privacy and are committed to protecting it through our compliance with this policy. This policy describes how we collect, process, retain, and disclose personal data about you when providing services to you through our websites, applications, products, and services that link to this policy (our “**Services**”) and our practices for using, maintaining, protecting, and disclosing that information.

This policy applies only to information we collect:

- Through the Services.
- In communications, including email, text, chat, and other electronic messages, between you and the Services.
- When you interact with our advertising and applications (including mobile apps) on third-party websites and services, if those applications or advertising include links to this policy.

It does not apply to information collected by:

- Us offline or through any other means, including on any other website operated by Sniffies or any third party (including our affiliates and subsidiaries) that does not link to this policy; or
- Any third party (including our affiliates and subsidiaries), including through any application or content (including advertising) that may link to or be accessible from or through the Services.

We may provide additional or different privacy policies that are specific to certain features, services, or activities.

Please read this policy carefully to understand our policies and practices regarding your information and how we treat it. By interacting with our Services or providing us with your information, you agree to the collection, use, and sharing of your information as described in this privacy policy. This policy may change on one or more occasions (see [Changes to Our Privacy Policy](#)). Your continued use of the Services after we make changes as described here is deemed to be acceptance of those changes, so please check the policy periodically for updates.

Sniffies is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

1. Children’s and Minors’ Data

Our Services are not intended for, and we do not knowingly collect any personal data from, children under the age of 18. If we learn we have collected or received personal data from a child under 18 years old without verification of parental consent, we will delete that information.

2. The Personal Data That We Collect or Process

“Personal data” is information that identifies, relates to, or describes, directly or indirectly, you as an individual, such as your name, email address, telephone number, shipping address, or payment information (for example, account information such as name, postal address, and email address).

The types and categories of personal data that we collect or process include:

- Account and contact information, including name, address (such as shipping address), email address, phone number, username, and other contact information you provide us.
- Payment information, including limited details about your payment method (such as the card type, expiration date, and billing ZIP code) as provided to us by our third-party payment processor and information about the payment methods and services (such as PayPal or Shop Pay) you use in connection with the Services. We do not collect or store your full credit or debit card number.
- Account history, including information about your subscription, account, transactions, purchases, order history, or discounts.
- Demographic information, including your age.
- Location information, including general geographic location such as country, state or province, or city.
- Device information, including your IP address, device identifiers, operating system and version, preferred language, hardware identifiers, browser type and settings, and other device information.
- Content and information you elect to provide as part of your profile or in any reviews you make through the Services or emails, chats, or other communications sent to us.
- Images, voice recordings, and videos collected or stored in connection with the Services.
- Biometric information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data, if you have consented to that information collection.

If you are a California resident, to access our supplemental California privacy statement, visit our [California Privacy Policy](#).

Some of the information identified above, including biometric information, may be considered sensitive data under certain laws. If required under applicable law, we will collect and process sensitive personal data only with your consent. If you choose not to provide or allow us to collect some information, we may not be able to provide you with requested features, services, or information.

We also collect:

- **Statistics or aggregated information.** Statistical or aggregated data does not directly identify a specific person, but we may derive non-personal statistical or aggregated data from personal data. For example, we may aggregate personal data to calculate the percentage of users accessing a specific Services feature.
- **Technical information.** Technical information includes information about your internet connection and usage details about your interactions with the Services, such as clickstream information to, through, and from our Services (including date and time), products that you view or search for; page response times, download errors, length of your visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), or methods used to browse away from a page.

If we combine or connect non-personal statistical or technical data with personal data so that it directly or indirectly identifies an individual, we treat the combined information as personal information.

3. How We Collect Your Personal and Other Data

You Provide Information to Us

We collect information about you when you interact with our Services, such as when you create or update an account, place an order, subscribe, make a purchase, participate in surveys, sweepstakes, contests, or promotions, or create, upload, or post content to the Services, including reviews, media such as photos, videos, or audio recordings.

Automatically Through Our Services

As you navigate through and interact with our Services, we may use automatic data collection technologies to collect information that may include personal data. Information collected automatically may include usage details, IP addresses, operating system, and browser type, and information collected through cookies, web beacons, and other tracking technologies including details of your interactions with our Services, such as traffic data, location data, logs, and other communication data, and which resources and Services features that you access and use.

We may use these automatic collection technologies to collect information about your online activities over time and across third-party sites or other online services (behavioral tracking).

Using automatic collection technologies helps us to improve our Services and to deliver a better and more personalized experience.

The technologies we use for this automatic data collection may include:

- **Cookies.** A cookie is a small file placed on your device when you interact with the Services. You may refuse to accept or disable cookies by activating the appropriate setting on your browser or device. However, if you select this setting, you may be unable to access certain features of the Services.

- **Web Beacons.** Some parts of the Services and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those parts or opened an email and for other related statistics (for example, recording the popularity of certain content and verifying system and server integrity). **We do not apply pixel tracking if you are in the EEA unless you have accepted the “Analytics” category for cookie consent.**

To the extent any of these automated technologies are considered a personal data sale, targeted advertising, or profiling, under applicable laws, depending on where you live, you may opt out from use of these automated technologies for such uses by contacting us at privacy@sniffies.com. Please note that some Services features may be unavailable as a result.

When you interact with the Services, there are third parties that may use automatic collection technologies to collect information about your or your device. These third parties may include:

- Advertisers, ad networks, and ad servers.
- Analytics companies.
- Your device manufacturer.
- Your internet or mobile service provider.

These third parties may use tracking technologies to collect information about you when you use the Services. The information they collect may be associated with your personal data or they may collect information, including personal data, about your online activities over time and across different websites, apps, platforms, and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content.

We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

From Business Partners and Service Providers

We may receive personal data about you from other sources and combine that with information we collect directly from you. For example, we may obtain information about you from service providers that we engage to perform services on our behalf, such as content delivery services, payment processors, and analytics, security and anti-fraud services.

If you purchase products from SniffiesHush.com, the checkout process is powered by Shopify. Information you provide at checkout—including your contact and payment information—is processed directly by Shopify in accordance with its [Privacy Policy](#) and [Terms of Service](#). We receive certain order-related information from Shopify, such as your name, email address, shipping details, and order contents, to fulfill your purchase.

4. How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal data, to:

- Provide you with the Services and any contents, features, information, products, or services that we make available through the Services.
- Fulfill and manage subscriptions, purchases, orders, deliveries, payments, returns, and exchanges.
- Fulfill any other purpose for which you provide it.
- Provide you with notices about your account or subscription, including expiration and renewal notices.
- Improve our Services, including by analyzing your information and creating aggregated data derived from your information) to develop, maintain, analyze, improve, optimize, measure, and report on our Services and their features and how users interact with them. Our analysis may include the use of technology like machine learning and large language models, which may include training these models or sharing with third parties for model training.
- Promote our Services, business, and offerings by publishing advertising on our own Services and by placing ads on third parties' services. We may use your information to model, segment, target, offer, market, and advertise our Services.
- Carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- Notify you when Services updates are available and about changes to any products or services we offer or provide through them.
- Use general location information (such as IP-based geolocation) to display your approximate position on the map and show nearby users or activity as part of the core functionality of the Services.
- Estimate your age using automated tools or analysis to help determine eligibility to access the Services, including to comply with applicable age verification and legal requirements.
- Moderate user-generated content to detect, prevent, or respond to illegal, abusive, or otherwise prohibited material, including through the use of automated tools and manual review where appropriate. This may include detecting spam, child sexual abuse material (CSAM), or content that violates our Acceptable Use Policy.
- Detect, prevent, and investigate fraud, security breaches, or other potentially prohibited, harmful, or illegal activity on or through the Services.
- Comply with applicable laws, legal obligations, and requests from law enforcement or

government authorities.

- Debug and identify errors that impair intended functionality of the Services.
- Facilitate the sale, shipment, and customer service related to merchandise or physical goods offered through SniffiesHush.com, including coordinating with third-party ecommerce and payment platforms such as Shopify, Shop Pay, or PayPal.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

The usage information we collect, whether connected to your personal data or not, helps us improve our Services and deliver a better and more personalized experience by enabling us to:

- Estimate our audience sizes and usage patterns.
- Store information about your preferences, allowing us to customize the Services according to your individual needs and interests.
- Speed up your searches.
- Recognize you when you return to our Services.

We may also use your information to contact you about goods and services that may be of interest to you. If you do not want us to use your information in this way, please adjust your use preferences in your account profile. For more information, see [Your Rights and Choices About Your Information](#).

We use location information we collect to display your approximate position on the map and show nearby users or activity as part of the core functionality of the Services. We do not collect or access precise location data (such as GPS data) from your device.

4.1 How we store and process your data

Your data will be collected, stored and processed securely. In case where we transfer your data internationally, we will ensure we take appropriate precautions to protect this data. Your data will normally be stored for up to 7 years in order to meet our legal obligations and protect our interests.

We will only use your personal data for the purposes for which it was collected unless we reasonably believe that another use is necessary and compatible with the original purpose. If you would like more information about the compatibility of a new purpose with the original purpose, please contact us. If we need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis for doing so.

In certain circumstances, we may be legally required to disclose your personal information without your knowledge. These circumstances include legal obligations, ongoing or

prospective legal proceedings, or to establish, exercise, or defend our legal rights. This may involve providing information to others for fraud prevention or credit risk reduction. We may also disclose information if we believe a court or other competent authority would likely order us to do so.

5. Automated Decision-Making and Profiling

We use automated decision-making, including profiling, in connection with our age estimation and content moderation processes. In some cases, these automated decisions may affect your access to certain Services or content. For example:

- **Age Estimation:** We may use automated systems to estimate whether you meet the minimum age requirements to access our Services. Where required by law, you may have the right to request a review of any age-related decisions that significantly affect you.
- **Content Moderation:** We use automated tools to help identify and moderate content that may violate our terms or applicable laws, including child sexual abuse material (CSAM), spam, or abusive content. While these decisions are generally subject to human oversight or appeal, certain content may be automatically restricted or removed in clear-cut or urgent cases.

We may also engage service providers that use artificial intelligence (AI) technologies to help identify content—such as photos or videos submitted by you or others—that may depict minors, human trafficking, CSAM, physical abuse, or other potentially unlawful or harmful material. These technologies rely on machine learning models that analyze and classify visual data. If that content is detected, it may be removed from our Services, and your account may be automatically suspended. In some cases, content flagged by AI may be reviewed by our human moderation team. We may also disclose your personal data to law enforcement or other authorities as required or permitted by applicable law.

Where required by law (including under GDPR Article 22), you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on you. You may also have the right to request human review or challenge the decision. If applicable, you may exercise these rights by contacting us at privacy@sniffies.com.

6. Who We Disclose Your Information To

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may also disclose personal data that we collect or you provide as described in this privacy policy:

- To our subsidiaries and affiliates.
- To contractors, service providers, and other third parties we use to support our organization and who are bound by contractual obligations to keep personal data confidential and use it only for the purposes for which we disclose it to them.

- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Sniffies's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by Sniffies is among the assets transferred.
- To fulfill the purpose for which you provide it.
- For any other purpose disclosed by us when you provide the information.
- With your consent.
- Sniffies is a location-based platform where certain user profile information is publicly visible by default. When you use the Services, other users may view your profile, including your username, general location, and any content you choose to share or post. Depending on how you use the Services, this may include sensitive personal data. While we provide certain settings to help limit visibility, we cannot guarantee complete privacy, and users may be able to infer your identity through your interactions or location. Do not include information in your profile that you wish to keep private.

We may also disclose your personal data:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request.
- To enforce or apply our Terms of Service or Terms of Sale and other agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our organization, our customers/users, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction. For example, we may disclose your personal data to your bank if you submit a dispute or chargeback against us for a purchase you have made on our Services.

The categories of personal data we may disclose include:

- Identifiers (such as email address, username, and device identifiers)
- Commercial information (such as subscription and order history)
- Payment information (limited details from our payment processor, such as card type and billing ZIP code)
- Internet or other electronic network activity (such as IP address, browser type, and usage data)

- Location data (such as general geographic location based on IP address)
- User-generated content (such as profile information, messages, reviews, or media you upload)
- Audio, visual, or similar information (such as voice recordings or videos, if provided)
- Biometric information (if you have consented to such collection)
- Inferences drawn from your information (such as aggregated usage patterns)

7. Cross-Border Data Transfers

We are based in the United States of America. We may process, store, and transfer the personal data we collect in and to countries outside of your own, including to jurisdictions that may not provide the same level of data protection as your country of residence.

If you are located in Canada, please note that personal data transferred outside of Canada may become accessible to foreign law enforcement or other authorities under the laws of those jurisdictions.

If you are located in the European Economic Area (EEA), Switzerland, or the United Kingdom (UK), your personal data may be transferred to countries outside of those regions, including to the United States. Where required by applicable law, we implement appropriate safeguards—such as standard contractual clauses approved by the European Commission or other lawful mechanisms—to ensure an adequate level of protection for your personal data. For more information about these safeguards, please contact us at privacy@sniffies.com.

8. Your Rights and Choices About Your Information

This section describes mechanisms you can use to control certain uses and disclosures of your information and rights you may have under state law, depending on where you live.

Advertising, marketing, cookies, and other tracking technologies choices:

- **Cookies and Other Tracking Technologies.** You can set your browser to refuse all or some browser cookies or other tracking technology files, or to alert you when these files are being sent. You can choose whether or not to allow the Services to collect information through other tracking technologies by configuring your browser settings to block or delete cookies and similar technologies. If you disable or refuse cookies or similar tracking files, some Services features may be inaccessible or not function properly. Some browsers include a “Do Not Track” (DNT) setting that can send a signal to the online services you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our Services may not respond to all browser DNT signals. Instead, you can use the range of other tools to control data collection and use, including the cookie controls and advertising controls described in this policy.
- **Promotions by the Company.** If you do not wish us to use your information used

to promote our own or third parties' products or services, you can opt out by logging into your account and adjusting your account settings and preferences or sending us an email stating your request to privacy@sniffies.com.

Location data choices:

- **Location Data.** The Services do not access precise, real-time location data (such as GPS) from your device. We determine your general location based on your IP address. Because location data is derived automatically from your connection, it cannot be disabled through device privacy settings. If you choose to use the map or location-based features of the Services, your approximate location will be visible to other users.

9. Your State Privacy Rights

Depending on your state of residency, you may have certain rights related to your personal data, including:

- **Access and Data Portability.** Confirm whether we process your personal data and access a copy of the personal data we process. To the extent feasible and required by state law, depending on your state, data will be provided in a portable format. Depending on your state, you may have the right to receive additional information and it will be included in the response to your access request.
- **Correction.** Request that we correct inaccuracies in your personal data that we maintain, taking into account the information's nature and processing purpose.
- **Deletion.** Request that we delete personal data about you that we maintain, subject to certain exception under applicable law.
- **Opt Out of Using Personal Data for Targeted Advertising, Profiling, and Sales.**
Request that we do not use your personal data for these purposes.

Important: The exact scope of these rights vary by state. There are also several exceptions where we may not have an obligation to fulfill your request.

To exercise any of these rights, please email us at privacy@sniffies.com. To protect your personal data from unauthorized access, change, or deletion, we may require you to verify your credentials before you can submit a request to know, correct, or delete personal data. If you do not have an account with us, or if we suspect fraudulent or malicious activity, we may ask you to provide additional personal data for verification. If we cannot verify your identity, we will not be able to honor your request. You may also submit a rights request through an authorized agent. If you do so, the agent must present signed written permission to act on your behalf and you may also be required to independently verify your identity with us. Authorized agent requests can be submitted to privacy@sniffies.com.

To appeal a decision regarding a consumer rights request, please send us an email at privacy@sniffies.com within 30 days after the decision was rendered with a detailed explanation of why you believe the decision was incorrect or unsatisfactory and any additional information or evidence that supports your appeal. On receipt of your appeal, we will acknowledge its receipt within ten business days. The appeal will be reviewed by a senior member of our data protection or compliance team who was not involved in the initial

decision. We may contact you for further information or clarification if necessary. We will provide a written response to your appeal within 30 days of receipt. If additional time is required to review your appeal, we will notify you of the extension and the reasons for it. If your appeal is upheld, we will take the necessary steps to rectify the issue and inform you of the actions taken. If your appeal is denied, we will provide a detailed explanation of the reasons for the denial and inform you of any further options available, such as contacting the relevant state authorities or data protection agencies.

Some browsers and browser extensions support the Global Privacy Control (“GPC”) that can send a signal to process your request to opt out from certain types of data processing, including data “sales” as defined under certain laws. When we detect such a signal, we will make reasonable efforts to respect your choices indicated by a GPC setting as required by applicable law.

Nevada provides its residents with a limited right to opt out of certain personal data sales. Residents who wish to exercise their sale opt-out rights may submit a request to this designated address: privacy@sniffies.com. However, please know we do not currently sell data triggering that statute’s opt-out requirements.

If you are a California resident, additional information applies to you. To access our supplemental California privacy statement and learn more about California residents’ privacy rights, visit our [California Privacy Policy](#).

10. Your EEA/UK Privacy Rights and Disclosures

If you reside in the EU, the EEA, Switzerland, or the UK, the following additional terms apply to our processing of your personal data.

Controller. Sniffies, LLC, with its registered office at 8 The Green, Suite B, Dover, Delaware 19901, is the controller and is responsible for the processing of your personal data as described in this privacy policy.

Legal Basis for Processing. We only process your personal data where applicable law permits or requires it, including:

- Where the processing is necessary for the performance of our contract with you.
- Where the processing is necessary for our legitimate interests or the legitimate interests of third parties. Where we rely on legitimate interest as the lawful basis for processing, we will conduct an appropriate assessment to ensure that such interests are not overridden by the rights and freedoms of data subjects.
- Where the processing is necessary to comply with a legal obligation, such as responding to a legal request or retaining transaction information to comply with record-keeping obligations.
- With your consent. For example, certain personal data processed by our Services may be considered “special category data” under article 9 of the GDPR, including data revealing sexual orientation or sexual behavior. We process this data only with your explicit consent or where necessary for reasons of substantial public interest, in accordance with applicable law.

What we use your personal data for:	Legal basis:
--	---------------------

To register you as a new customer	Performance of a contract with you
To send you account-related notices, including expiration and renewal notices	For the performance of our contract with you To comply with our legal and regulatory obligations
To estimate your age using automated tools or analysis	To comply with our legal and regulatory obligations
To provide products or services to you, including to process and deliver your order; to manage payments, fees, and charges; and to collect and recover money owed to us	For the performance of our contract with you or to take steps at your request before entering into a contract Necessary for our legitimate interests (to recover debts due to us)
To prevent and detect fraud against you or Sniffies	For our legitimate interests or those of a nonparty, i.e., to minimize fraud that could be damaging for us and for you
To moderate our Services for child sexual abuse material (CSAM) and other illegal content, including through automated decision-making and account restrictions	For our legitimate interests or those of a third party, that is, to prevent and detect CSAM that could be damaging for us and for you To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, e.g., policies covering security and internet use	For our legitimate interests or those of a third party, i.e., to make sure we are following our own internal procedures so we can deliver the best service to you
Operational reasons, including improving efficiency, training, and quality control	For our legitimate interests or those of a third party, i.e., to be as efficient as we can so we can deliver the best service for you at the best price
Statistical analysis to help us manage our business, e.g., for customer base or other efficiency measures	For our legitimate interests or those of a third party, i.e., to be as efficient as we can so we can deliver the best service for you at the best price

Preventing unauthorized access and modifications to systems	For our legitimate interests or those of a third party, i.e., to prevent and detect criminal activity that could be damaging for us and for you To comply with our legal and regulatory obligations
Updating customer records	For the performance of our contract with you or to take steps at your request before entering into a contract To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g., making sure that we can keep in touch with our customers about existing orders and new products
Marketing our Services to existing and former customers and to third parties who have previously expressed an interest in our Services	For our legitimate interests or those of a third party, i.e., to promote our business to existing and former customers
To assist law enforcement and response to subpoenas	To comply with our legal and regulatory obligations
To promote our Services by placing ads on our own or third-party platforms and tailoring offers or content	For our legitimate interests or those of a third party, i.e., to market our business and offerings to potential and current users

Your legal rights. Under certain circumstances, you have rights under data protection laws in relation to your personal data. Your rights might include the following:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us to continue to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully, or where we are required to erase your

personal data to comply with local law. Note, however, that we might not always be able to comply with your request of erasure for specific legal reasons that will be notified to you, if applicable, at the time of your request.

- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information that override your rights and freedoms.
- **Request restriction of processing** your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful, but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise, or defend legal claims; or (d) you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer** of your personal data to you or a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information that you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we might not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Exercising Your Rights. If you wish to exercise any of the rights set out above, please contact us at privacy@sniffies.com.

Fees. You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to honor your request in these circumstances.

Verification. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information regarding your request to speed up our response.

Responding to Your Request. We try to respond to all legitimate requests within one month. Occasionally, it may take us longer than a month if your request is particularly complex or you have made several requests. In this case, we will let you know and keep you updated.

Right to Lodge Complaint. If you believe our data processing practices violate your rights under the EU or UK GDPR, you may lodge a complaint with the supervisory authority in your country of residence or work. If you are in the EU, you can find your local supervisory authority [here](#). For any unresolved complaints relating to the UK, you can reach out to the [Information Commissioner's Office](#), and for Switzerland, to the [Federal Data Protection and Information Commissioner](#). While you have the right to lodge a complaint directly with the supervisory authority, we welcome the opportunity to address your concerns and resolve any issues first.

11. Our Obligation under the GDPR

We take the responsibility of the management and security of your personal data extremely seriously. In accordance with the General Data Protection Regulation, acting as a data controller and data processor, we follow the key principles of data protection. These require that personal data be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up to date. Every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

12. How We Protect Your Personal Data

We use commercially reasonable administrative, physical, and technical measures designed to protect your personal data from accidental loss or destruction and from unauthorized access, use, alteration, and disclosure. However, no website, mobile application, system, electronic storage, or online service is completely secure, and we cannot guarantee the security of your personal data transmitted to, through, using, or in connection with the Services. In particular, email, texts, and chats sent to or from the Services may not be secure, and you should carefully decide what information you send to us via those communications channels. Any transmission of personal data is at your own risk.

The safety and security of your information also depends on you. You are responsible for taking steps to protect your personal data against unauthorized use, disclosure, and access.

12. How We Retain Your Personal Data

We keep the categories of personal data described in this policy for as long as reasonably necessary to fulfill the purposes described or for as otherwise legally permitted or required, such as maintaining the Services, operating our organization, complying with our legal obligations, resolving disputes, and for safety, security, and fraud prevention. This means that we consider our legal and business obligations, potential risks of harm, and nature of the information when deciding how long to retain personal data. At the end of the retention period, personal data will be deleted, destroyed, or deidentified.

We may retain limited, non-reversible or tokenized identifiers derived from contact, device, network, or behavioral signals (e.g., hashed email, server-issued security tokens, hashed/truncated IP signals) after account closure solely to detect and prevent fraud or abuse—including attempted re-registration following serious policy violations—in line with our data-minimization and retention practices. We do not retain raw contact details for this purpose, and we do not use these identifiers for advertising or cross-app tracking

If you are a California resident, visit our [California Privacy Policy](#) for more information about the retention periods that apply to the personal data categories we collect.

13. Changes to Our Privacy Policy

We may update this policy on one or more occasions, and we will provide notice of any such changes to the policy as required by law. The date the privacy policy was last updated is identified at the top of the page. We will notify you of changes to this policy by updating the “last updated” date and posting the updated policy on the Services. We may email or otherwise communicate reminders about this policy, but you should check our Services periodically to see the current policy and any changes we have made to it.

14. Contact Information

To exercise your rights or ask questions or comment about this privacy policy or our privacy practices, contact us at: privacy@sniffies.com.

Due to the nature of our business and our processing activities, we are qualified to appoint a Data Protection Officer, as stipulated in Article 37 of the GDPR. Our DPO is:

GDPR Local Ltd
Adam Brogden
dpo.support@gdprlocal.com
Tel + 441 772 217 800
GDPR Local Ltd

1st Floor Front Suite 27-29 North Street, Brighton, England BN1 1EB

We have procedures in place to receive and respond to questions, complaints, or inquiries about our handling of personal data and our compliance with this policy and applicable privacy laws. To raise a concern or contact us about our privacy practices, please use the contact information provided above.

Article 27 Representative

We have appointed EU and UK Representatives under Article 27 of the EU GDPR and UK

GDPR respectively. Our appointed representatives are:

Our UK Representative:

Under Article 27 of the UK Data Privacy Act, we have appointed a UK Representative to act as our data protection agent. Our nominated UK Representative is: GDPR Local Ltd.

Adam Brogden
contact@gdprlocal.com
Tel: +44 1772 217800
1st Floor Front Suite
27-29 North Street, Brighton
England
BN1 1EB

Our EU Representative:

Under Article 27 of the GDPR, we have appointed an EU Representative to act as our data protection agent. Our nominated EU Representative is: Instant EU GDPR Representative Ltd.

Adam Brogden contact@gdprlocal.com
Tel +35315549700
INSTANT EU GDPR REPRESENTATIVE LTD
Office 2,
12A Lower Main Street, Lucan Co. Dublin
K78 X5P8
Ireland