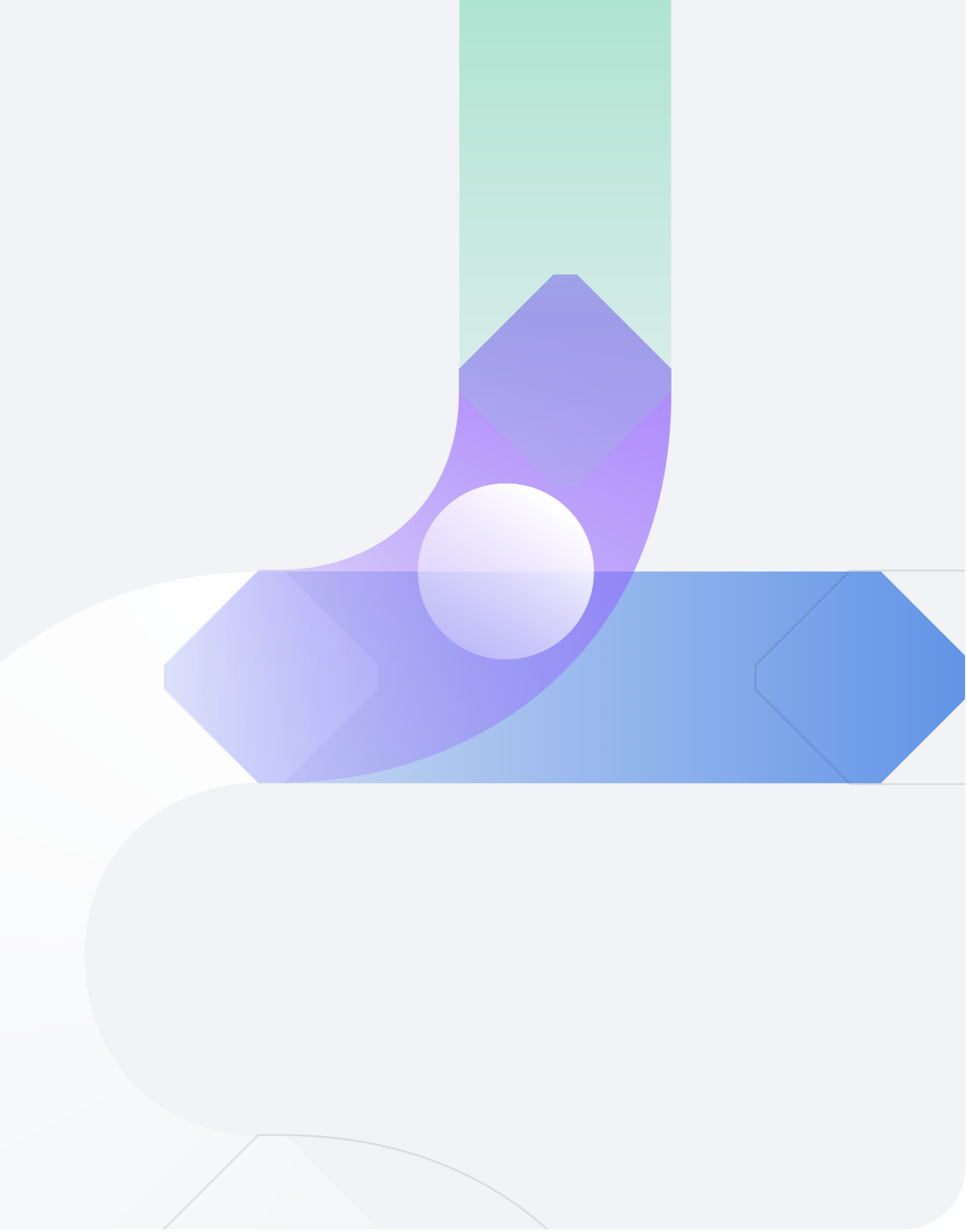


Individual Privacy Policy

cloudsmith

cloudsmith

Individual Privacy Policy

1. Our Policy

Security and privacy are paramount at Cloudsmith, both implementing and protecting it. Our mission has always been to offer world-class expertise and support for package management while building a service you can genuinely trust, backed up by our self-imposed Tao of integrity and transparency. We believe it is possible to do this without treating you or your customers as assets to be traded or sold.

We'll do so when you want us to serve your information publicly. When you want it to remain private, we endeavor to keep it that way. Otherwise, we will only use your information in the ways we've promised here in this privacy policy, such as providing or improving the Service, sending you marketing and other materials only when you want it, and providing incredible support. Data collection has a purpose: never to line our pockets by capitalizing on the data. Your data is yours, and we want to keep it that way.

Therefore, our promise to you is to:

- Respect Your Boundaries (only collect/use what is necessary);
- Protect Your Data (keep it safe and secure); and
- Avoid Dark Patterns (don't use data unnecessarily, such as selling it for profit).

2. Introduction

This privacy policy informs you about how we look after your data and Personally Identifiable Information (**PII**). The privacy policy applies when you interact with us as one of our users or access our sites and services, including our data and package management software services, marketed under the Cloudsmith® trademark. It also applies where you are a supplier or business partner who interacts with us for business purposes. Separate policies apply to our processing of PII where you are a Cloudsmith employee or job applicant. It also informs you about your privacy rights and how the law protects you. It does not cover any third-party website you have used to access our websites or services or any third-party websites you access from them.

We may amend this Policy from time to time, as in Section 17 below. We will provide you with at least twenty-eight (28) days' notice before making a material (i.e., non-typographic) change. Every time you subscribe for an account with us or use our services, you should check the latest version of this Policy to ensure that you understand what terms will apply. This Policy was last updated on **23 June 2022**. Historic versions can be obtained by contacting us.

3. Section Summary

If we collect your PII, we do so only with your consent to provide you with services you have signed up for or when acting in our legitimate interests that do not override your rights or freedoms. We only collect the minimum amount of PII necessary to fulfill the purpose of your interaction with us. We don't sell your PII to third parties; we only use it as outlined in this Policy. This processing applies regardless of who you are and wherever and whenever you access our sites or services.

We have provided a quick summary of this Policy's relevant sections below, with links to the relevant sections. These summaries obviously can't cover everything, so please make sure you read the rest of this Policy so that you are fully aware of how and why we are using your data.

This Policy includes our cookies and technologies policy in Appendix 1 below, a series of disclosures specifically relevant to our services' customers in Appendix 2 below, and, if you are a California resident, our California Consumer Privacy Act 2018 notice in Appendix 3 below.

Section	Summary
Who Is Cloudsmith?	Confirms our company details and sets out at a high level the different capacities we process your PII, i.e., when we typically decide how to process your data and what to process it for when we process it per your instructions.
What Kind Of PII Does Cloudsmith Process?	Generally, you may provide PII to us when you register to use our services, upload it using our services, communicate with us, or transact with us. We will also automatically collect technical data about your use of our website and services using cookies and similar technologies and device information, subject, where necessary, to your consent (you may be identifiable from such data where logged in at the time). We may also collect PII from third parties. We only collect the minimum amount of PII necessary from you unless you choose to provide more.
What Information Is Not Collected?	We do not knowingly collect PII from/about children under 16 or sensitive PII. We ask that you don't upload sensitive PII (for example, financial data or medical information) using our services. Additionally, you must have permission to share any PII relating to third parties you may share with us.
How is Your Information Used?	We use PII for various reasons, including providing our services, security and compliance, and improving our services and website(s). We set out the legal basis for processing your information in this section. If we collect your PII, we do so only with your consent or to provide you with services you have signed up for or act in our legitimate interests that do not override your legitimate rights or freedoms.
What Information Is Shared?	We may share your information with third parties under one of the following circumstances: with your consent, with our service providers, for security purposes, to comply with our legal obligations (e.g., with relevant governmental or regulatory authorities), with other users within the organization with which your account is affiliated, or when there is a change of control or sale of our company or business. We do not sell your PII, and we do not host advertising on our website(s) or platforms. We require all relevant third parties to respect your PII's security and treat it per the law.
Is Publicly Available Information Treated Differently?	If the PII you upload using our Services is in public directories/packages (which you can opt-in or out of at any time), third parties may access and use it in compliance with our Terms of Service.
How Is My Information Secured?	We take all measures reasonably necessary to protect PII from unauthorized access, alteration, or destruction, maintain its accuracy, and help ensure its appropriate use, following accepted industry standards where possible boring transmission and once we receive it. For further information, please see our Security Policy.
How Is Information Collected And Stored Globally?	PII we hold is stored and processed in the UK, EU, and (less-so) USA per this Policy. While we provide the same standard of privacy protection to all our users around the world, regardless of their country of origin or location, we understand that we have users from different countries and regions with varying expectations of privacy and local legal requirements, and we try to meet those needs and requirements.

Section	Summary
What Happens If I Have A Complaint?	If you have concerns about how we have handled your PII, we would be happy to discuss independent arbitration services.
How Does Cloudsmith Respond To Compelled Disclosure Requests?	We may disclose PII or other information we hold about you to law enforcement bodies in response to a valid regulatory order or when we believe in good faith that disclosure is reasonably necessary to protect our property or rights, those of third parties, or the public at large. We strive for transparency in replying to such requests where possible.
How Can I Access My PII?	We provide ways for you to access, alter, or delete your PII. If you're already a Cloudsmith user, you may access, update, change, or delete your basic user profile information by editing your user profile or contacting us, for example.
How Long Is PII Retained For Before Deletion?	We will only retain your PII for as long as necessary to fulfill the purposes we collected it for, including to satisfy any legal, accounting, or reporting requirements.
How Does Cloudsmith Communicate With Users?	We may contact you either by e-mail or within our services, typically around changes in a package repository you're watching, new features, requests for feedback, significant policy changes, or to offer customer support. We also send marketing e-mails, but only with your consent. You can control how we contact you in your account settings or by contacting us.
Will This Privacy Policy Change?	If there are material changes to this Policy or how we use your PII, we will prominently post such changes before implementing the change. We endeavor to give you advance notice before any such changes become effective. You may obtain historic versions by contacting us.
How Can I Contact Cloudsmith?	Please contact us if you have any questions about this Policy or our PII practices.
Appendix 1 - How we Use Cookies and Similar Technologies	We use cookies and similar technologies for our website(s)' overall functionality and a small number of tracking and analytics services on a few parts of our site. This Appendix details our use of cookies and similar technologies.
Appendix 2 – Third-Party Service Providers	We may share your PII with our third-party service providers, as noted above and in the relevant sections below. This Appendix provides more detail on the third-party service providers we partner with, the kinds of PII they may gain access to, and what they do with it.
Appendix 3 – CCPA Privacy Notice	This Appendix sets out a specific and more detailed privacy notice for California residents whose PII we process. It is not relevant to you if you reside elsewhere.

4. Who is Cloudsmith?

Under the EU and UK General Data Protection Regulations and other relevant data protection laws, we act as a data controller (i.e., where we make decisions concerning PII that we collect) and a data processor (i.e., where we process that PII according to your instructions).

When we act as a Data Processor: When you use our services to process PII in your content/packages, we act as a data processor. As a user, you can use the controls available in our services to handle any PII in that content. Under these circumstances, you or the company you work for will act as a data controller or data processor, and we will act as either a processor or a sub-processor.

When we act as a Data Controller: By contrast, when we collect PII and determine the purposes and means of processing that PII – for example, when we store account information for account registration, administration, services access, or contact information as explained below – we act as a data controller.

Contact Details

Our full details are:

Full Name of Legal Entity: Cloudsmith Ltd, a company incorporated in Northern Ireland under registered company number NI653568

Postal Address: Cloudsmith Ltd, Scottish Provident Building, 7 Donegall Square West, Belfast, BT1 1JH

Third-Party Links

Our websites and Services may include links to third-party websites, widgets, plug-ins, and applications (including various social media platforms). Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. However, we have attempted to provide high-level details about third-party platforms our websites and Services integrate, as described in Appendix 2 below. When you leave our website, we encourage you to read the Privacy Policy of every website you visit.

5. What kind of PII does Cloudsmith process?

Information You Supply To Us

General PII - This is PII about you that you share with us by online forms on our website, through e-mail, through the post, on the telephone, when you register to use our services or engage with our services, when you complete customer surveys, engage with our customer services team, deal with us as a supplier or business partner or by any other means.

Typically, when you deal with us, you may provide information about yourself and other data about your business, including your full name, job title, billing address, business name, personal or business e-mail address, telephone or mobile phone number, and other contact details. You may provide similar information or sign up for our newsletter when contacting us.

When signing up for our Services, you must provide your name and e-mail address. It also includes information you provide when you report any technical or service issues concerning our websites or Services, including relevant notes about any problems and how we responded to resolve these, as well as details of any payments you have made through our websites.

Customer Data: Any PII you upload when using our Services.

Financial Details: We may collect financial details where you pay for our services. Financial details of our customers include credit card numbers, sort codes and account numbers, and billing information. We do not process or store your credit card or financial account information, but our third-party payment processor does. Such payment processors are not permitted to store, retain, or use the information you provide except for processing payments on our behalf.

When you pay for a product or service via bank transfer, we may ask you to provide information to facilitate this transaction and verify your identity.

Verbal Information: If you provide PII verbally that you give us consent to use, you will have such consent confirmed back to you in writing.

Marketing Information: You may also communicate your preferences in receiving marketing from us and our third parties and your communication preferences (including details you provide when you opt-in to receive marketing communications from us).

Third-Party Data: Where you are sharing PII that does not directly relate to you (e.g., your representatives that legally act on your behalf), you must ensure you have the consent to do so and have shared this Policy with that person/those people, including where you are acting to register other individuals on their behalf.

Suppose You Fail To Provide PII

Where we need to collect PII by law or under the terms of a contract we have with you, you failed to provide that data when requested. In that case, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with products). In this case, we may not be able to fulfill any order you place with us, but we will notify you if this is the case at the time.

PII We Collect

Telephone Recordings - We may record telephone conversations for training or monitoring purposes.

Technical Data from our Websites: we use certain technical services to gather technical data online whenever you use our websites, including information about your device and your visits to our websites, such as your IP address, geographical location, browser type, referral source, length of stay and pages viewed. Please see our cookies and similar technologies Policy in Appendix 1 below for further details.

Technical Data from our Services: we also use certain technical services to gather technical and usage data whenever you use our Services, including device, content, and usage data. We collect this data using cookies and other similar technologies. Please see our cookie and similar technologies policy in Appendix 1 below for further details.

PII We Receive From Third Parties

We may collect PII. For example:

- **Device Data:** analytics providers such as Google based outside the EU; advertising networks such as Google based outside the EU and RollWorks based outside the EU; and search information providers such as Google based outside the EU.
- **Contact, Financial and Transaction Data:** from providers of technical, payment, and delivery services such as Stripe outside the EU and Intercom inside the EU.
- **Social Media:** publicly available information through social media sites, such as Facebook, LinkedIn, Twitter, Instagram, YouTube, and Google, including where you have responded to a promotional item or offer from us through social media facilities.
- **Publicly Available Information:** we may collect PII about you from other publicly available sources. This PII can include your name, address, and additional publicly available information.
- **Customer Data:** Our customers may collect, store, and process PII about you through our services. We have requested that no special categories of PII (such as financial Information, medical data, and Information about religious or political opinions) are collected through our services. Still, otherwise, we do not control our customers' use or processing of PII through our services.
- **Other Examples:** This may happen if you sign up for training or to receive information about us from one of our vendors, partners, or affiliates. We do not purchase PII from third-party data brokers.

IMPORTANT – PLEASE NOTE: Our Terms of Service require our customers to refrain from uploading or processing any data using our Services in violation of applicable laws, including not to process any PII without valid legal grounds, not to process any sensitive or special categories of data (such as financial Information, medical data, Information about religious or political affiliations) and not to infringe any third party's other rights using our Services.

We require all our customers to agree to adhere to these terms at all times but do not actively monitor content uploaded or processed using our Services and are not responsible for enforcing those terms. Don't hesitate to contact us if you review this Policy because you believe your or your organization's data has been used to violate those terms.

Keeping Your PII Accurate

The data we hold about you must be accurate and current. Please keep us informed if your PII changes during your relationship with us.

6. What information is not collected?

We do not intentionally collect "**sensitive personal information**" or special category data (including details about your race or ethnicity, religious or philosophical beliefs, medical information, sex life, sexual orientation, political opinions, trade union membership, genetic and biometric data, social security numbers). Nor do we collect any information about criminal convictions and offenses.

As noted above, our Terms of Service include restrictions on our customers using our Services to collect such data (or financial information). As stated, we do not proactively monitor this and cannot be held responsible when our customers breach these restrictions.

If you're a child under 16 (or are otherwise legally regarded as a child in your country of residence), you may not have an account on Cloudsmith. Cloudsmith does not knowingly collect information from or direct any of our content to children under relevant ages. If we learn or have reason to suspect that you are a user who meets these criteria, we will, unfortunately, have to close your account. Please see our Terms of Service for Information about account termination.

7. How is your information used?

We will only use your PII when relevant law allows us to. To the extent that our PII processing is subject to specific international laws (including the EU and UK General Data Protection Regulations), we must notify you about the legal basis on which we process that PII. Most commonly, we will process your PII in the following circumstances where:

- We need to perform the contract we are about to enter into or have entered into with you to keep internal records for administrative purposes related to such agreements, for the purposes contemplated in any separate terms of use for our websites that you have entered into, including for the purposes set out in the "Our Standard Business Operations" section below; which are the grounds we rely upon to process Customer Data our customers upload when using our Services;
- It is necessary for our legitimate interests (or those of a third party), and your interests and fundamental rights do not override those interests; or
- We need to comply with a legal or regulatory obligation.

Generally, we do not rely on consent as a legal basis for processing your PII other than as set out below concerning marketing and testimonials. We may process your PII for more than one lawful ground depending on the specific purpose of using your data.

Our Standard Business Operations:

Some examples of our standard business operations are set out below:

- To provide our services that we contract to deliver to you or to the relevant Customer to whom we sell access to our services and who has authorized you to access the same on their behalf;
- To receive products and services from you as a supplier or to administer our business relationship with you;
- To provide you with the information that you request from us;
- To confirm your identity as a natural living person;
- To comply with our legal obligations, protect our intellectual property, enforce our Terms of Service; and
- As part of our billing, payments, and recovery processes.

We may also use contact information to notify you of any issues that impact our services' provision.

Marketing

We maintain multiple contact lists (with e-mail addresses and other information) to communicate with individuals who do business with us or express an interest in our services.

We may contact you to confirm your purchases or respond to requests that you make, notify you of changes to your account or our services for marketing purposes, or otherwise inform you of information related to our business or your account with us.

You will only receive marketing communications from us if you have opted to receive them, including where you have consented to be contacted by us by e-mail or telephone. You can opt-in over the phone, by e-mail, or online. We strive to provide you with choices regarding PII uses for marketing and advertising and currently use this to manage our e-mail correspondence. You can ask us to stop sending you marketing messages by following the opt-out links on any marketing message sent to you or by contacting us, as appropriate, at any time.

Testimonials

We may post customer testimonials and comments on our websites or other platforms, which may contain PII. Before posting the customer's name and testimonial, we obtain each customer's consent via e-mail.

Change of Purpose

We will only use your PII for the purposes we collected it unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. Don't hesitate to contact us if you wish to explain how the new purpose's processing is consistent with the original purpose.

If we need to use your PII for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. Please note that we may process your PII without your knowledge or consent in compliance with the above rules, where this is required or permitted by law.

Legal Requirements

We will keep and use your data regarding any legal or regulatory requirements. We can use your data to protect our legal position if legal action is required, including resolving any outstanding debts. By way of example, we will share your PII with the relevant agencies without notice where we are requested to or suspect fraudulent activities, money laundering, and terrorism-related activities.

Customer Data

While we have access to PII stored in your package repositories or other free-form content inputs, we do not process such data unless per your instructions and this Policy. Information in your package repositories belongs to you, and you are responsible for ensuring that your content complies with our Terms of Service.

Private Customer Data: We do not access any information (including PII contained in same) in private packages unless required for security or maintenance, or support reasons, or to enforce or defend our rights, to comply with the law, or with the consent of the package repository owner, or process it other than to store the data securely as described herein and per this Policy, and then delete it as applicable.

However, while we do not generally search for content in your packages, we may scan our servers and content to detect specific tokens or security signatures, known malicious code, or other content known to violate our Terms of Service, such as violent extremist or terrorist content or child exploitation, as detailed in our Terms of Service.

Public Customer Data: If your package repository is public, anyone (including us) may view its contents. Suppose you have included private or sensitive information in your public (shared) package repository, such as e-mail addresses. In that case, that information may be indexed by search engines or used by third parties.

Enhancing our Services

We may use PII (other than that composed of private Customer Data) to provide or improve our IP geolocation, fraud detection, demographic targeting, and other Services and products.

Website Administration and Customisation

We may use the information we collect about you for various website administration and customization purposes. For example, we use your information to process your registration request, provide you with services and communications that you have requested, send you updates via e-mail and other communications, customize features and advertising that appear on our websites, and deliver our website content to you, measure website traffic, measure user interests and traffic patterns, and improve our websites and our services and features offered via our websites.

Aggregated or Non-Identifying Information

Non-identifying information includes information collected from or about you that does not personally identify you – including aggregated information. We may use non-identifying information for any purpose.

We may also combine your non-identifying information with third-party data sources (including data obtained from offline sources and data received from our customers using our services) to improve our Services. We may share such non-identifying information with customers, affiliates, and third parties.

Certain jurisdictions, including the European Union, may deem IP addresses or Unique IDs PII. Accordingly, our use of Non-Identifying Information described in this Policy should not be assumed to include IP addresses and Unique ID data for persons in such jurisdictions.

8. What information is shared?

We do not disclose PII outside Cloudsmith, except in the situations listed in this section or sections below on Compelled Disclosure. Still, we may have to share your PII with the categories of data processors or data controllers set out below for the purposes set out in the above or otherwise below:

- With third parties, with your permission. We may infer consent directly or indirectly from your actions when using the Cloudsmith platform. For example, this includes other users within the organization with which your account is affiliated, who can access all information you input, store, or process using our services (by associating your account with an organization, you indicate your willingness to provide the owner of the organization with the ability to view your activity in the organization's access log);

- With organizations with whom your account is associated, or purported to be associated, for security purposes; this might include sharing your username, e-mail, usage information, and device information with that organization with an owner or administrator of the organization, to the extent that such information is provided only to investigate or respond to a security incident that affects or compromises the security of that particular organization;
- With HM Revenue & Customs, regulators and other authorities who require reporting of processing activities in certain circumstances;
- With third-party purchasers, if we buy, sell or merge any business or assets of our company and are required to share data as part of the buying, selling, or merger agreement or if our assets are acquired by a third-party, and data is transferred as part of the purchased assets. This also applies to a potential purchase, sale, or merger and a potential or actual investment into our business. If any such change happens, we will ensure that it is under terms that preserve your PII's confidentiality. We will notify you on our website or by e-mail before any transfer of your PII where practicable. Any purchaser would be bound by the terms of this Policy and our Terms of Service;
- With professional advisers, including lawyers, bankers, auditors, and insurers who provide consultancy, banking, legal, insurance, and accounting services, where they need to know the same for any of the purposes set out above;
- With reputable and trusted third parties where we have asked them to contact you on our behalf, where you have given us consent, it is part of our contractual agreement, is a legal requirement, or there is clear legitimate interest between us (these services may include sending you an e-mail, calling you by telephone, or sending you information through the post);
- We may provide co-marketing content that we think may be relevant to you with trusted third parties where you have opted to receive such content. When you engage with these co-marketing partners, we will tell you whom we are sharing data with and link to the co-marketing partner's Privacy Policy to learn more about opting out of the partner's communications. These co-marketing partners are required to adhere to our privacy and data protection policies;
- With specific selected third parties, determined by us, if you breach any agreement with us, including to enforce our rights against you, including credit-reference agencies, debt-collection firms or service providers, solicitors or barristers, and law enforcement agencies (if applicable); and
- With service providers acting as processors based in the EU, USA, or UK (but who may process your PII outside of those jurisdictions) who provide technology and system administration services, including for the performance of our contract with you, as set out below (and as more particularly detailed in Appendix 2. When we transfer your data to our service providers, we remain responsible for it:
    a. With e-mail marketing services to send marketing e-mails where you have opted for receiving them. You can unsubscribe directly from any mailing list using the unsubscribe links provided within e-mails;
    b. With analytical service providers to analyze our website's traffic to improve products and services;
    c. With processors offering software tools, or EU or UK-based external servers (including externally provided original and backup servers) that are used to store PII provided by you on our behalf; and
    d. When processing payments, customer support ticketing, and transmitting data to other similar providers.

It is our policy to only disclose the Customer Data in your private packages to the extent necessary to provide you with the services you purchased from us; as part of the sale of our business, to enforce our legal rights, or to comply with our legal obligations.

We require all third-party service providers to respect your PII's security and treat it per the law. We do not allow our third-party service providers to use your PII for their purposes and only permit them to process the minimal PII required for the specified purposes, per our instructions, where they have agreed to privacy restrictions similar to our Policy.

We do not share, sell, rent, or trade PII with third parties for commercial purposes. The California Consumer Privacy Act of 2018 requires us to state whether we disclose PII in exchange for monetary or other valuable considerations. While CCPA only covers California residents, we extend its core rights around controls on the sale of their data to all of our users, not just those who live in California.

We share certain aggregated, non-personally identifying information with others about how our users, collectively, use Cloudsmith or how our users respond to our other offerings, such as our conferences or events. For example, we may compile statistics on the usage of package formats on Cloudsmith. However, we do not sell this information to advertisers or marketers.

9. Is publicly available information treated differently?

Much of our Services are public-facing by nature. If the Customer Data you process using our Services is public-facing, third parties may access and use it according to our Terms of Service. We do not sell that content; it is yours. However, we allow third parties, such as research organizations or archives, to compile public-facing Customer Data. If you do not want your PII to appear in third parties' compilations of Customer Data, please do not make your Customer Data publicly available.

If you would like to compile Cloudsmith's Customer Data, you may only use any public-facing Customer Data you gather for the purpose our user has authorized it. For example, where a Cloudsmith user has published a public-facing e-mail address for identification and attribution, do not use that e-mail address for commercial advertising. You must secure any Customer Data you have gathered from Cloudsmith and respond promptly to complaints, removal requests, and Do Not Contact requests from Cloudsmith or Cloudsmith users.

Similarly, package repositories on Cloudsmith may include publicly available Customer Data collected as part of the collaborative process. Suppose a Cloudsmith project contains publicly available Customer Data that does not belong to Cloudsmith users. In that case, we will only use that Customer Data for the limited purpose for which it was collected, and we will secure any PII contained in such Customer Data as we would secure any PII. If you have a complaint about any PII on Cloudsmith, please see our section on resolving complaints.

10. How is my information secured?

Cloudsmith takes all measures reasonably necessary to protect PII from unauthorized access, alteration, or destruction, maintain data accuracy and help ensure the appropriate use of PII. We follow generally accepted industry standards to protect the PII we hold during transmission and once we receive it.

Also, we limit access to your PII to those employees, agents, contractors, and other third parties who have a business need to know. They will only process your PII on our instructions, and they are subject to duties of confidentiality.

We have procedures to deal with any suspected PII breach and notify you and any applicable regulator of a breach where we are legally required to do so.

No method of transmission, or method of electronic storage, is 100% secure. Therefore, we cannot guarantee its absolute security. For more information on the measures we take to secure your PII, please see our Security Policy.

11. How is information collected and stored globally?

Information we collect will be stored and processed in the United States, the United Kingdom, and the European Union. However, we understand that we have users from different countries and regions with varying expectations of privacy and local legal requirements, and we try to meet those needs and requirements.

We provide the same standard of privacy protection to all our users worldwide, regardless of their country of origin or location. We are proud of the transparency, security, and accountability levels we provide. We work hard to comply with the applicable data privacy laws wherever we do business. Additionally, we require that if our vendors or affiliates have access to PII, they must comply with applicable data privacy laws.

We process PII inside and outside the UK and EU and rely on Standard Contractual Clauses as the legally provided mechanism to lawfully transfer data from the UK and EU to the USA and Australia.

In particular:

- We ensure there is an appropriate basis for processing any PII (including but not limited to a contractual obligation or legitimate interest);
- We collect only the minimum amount of PII necessary unless you choose to provide more. We encourage you only to give us the amount of data you are comfortable sharing;
- We offer you simple methods of accessing, correcting, or deleting the data we have collected; and
- We provide our users with notice, choice, accountability, security, and access. We limit the processing purpose and provide our users with a method of recourse and enforcement.

12. What happens if I have a complaint?

Please let us know if you have concerns about how Cloudsmith handles your PII. We want to help, and there are several ways available that you can contact us. You may also e-mail us at privacy@cloudsmith.io with the subject line “Privacy Concerns.” We will respond within ten working days at the latest. We would be happy to discuss independent arbitration services if we cannot resolve your concerns after a reasonable faith effort to address them.

Suppose you are a data subject based in the UK or European Union. In that case, you may have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk), or other competent supervisory authority of an EU member state if our services are accessed outside the UK. We would appreciate the chance to deal with your concerns before approaching such bodies, so we would ask that you please contact us in the first instance.

13. How does Cloudsmith respond to compelled disclosure requests?

Cloudsmith may disclose PII or other information we collect about you to law enforcement or regulatory bodies as required by law or in response to a valid subpoena, court order, warrant, or similar governmental order, or when we believe in good faith that disclosure is reasonably necessary to protect our property or rights, or those of third parties or the public at large.

In complying with court orders and similar legal processes, Cloudsmith strives for transparency. We will make a reasonable effort to notify users of any disclosure of their information unless the law or court order is prohibited from doing so or in rare, exigent circumstances.

14. How can I access my PII?

If you’re already a Cloudsmith user, you may access, update, alter, or delete your basic user profile information by editing your user profile or contacting us.

Under certain circumstances, where you are a European Union or UK citizen, you have rights under data protection laws concerning your PII under GDPR. You have the right to:

- **Request access** to your PII (commonly known as a “data subject access request”). This request enables you to receive a copy of the PII we hold about you and check that we are lawfully processing it.
- **Request correction** of the PII that we hold about you. This request enables you to have any incomplete or inaccurate data we hold about you corrected. However, we may need to verify the accuracy of the new data you provide.
- **Request erasure** of your PII. This request enables you to delete or remove PII 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 PII 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 PII to comply with local law. However, please note that we may 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** your PII where we rely on a legitimate interest (or those of a third party). This request enables you to object to processing where you feel it impacts your fundamental rights and freedoms. You also have the right to object to where we are processing your PII for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

- **Request restriction of processing** of your PII. This request enables you to ask us to suspend the processing of your PII 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 PII to you or a third party. We will provide you, or a third party you have chosen, your PII in a structured, commonly used, machine-readable format. Note that this right only applies to automated information 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 PII. However, this will not affect the lawfulness of any processing before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case when you withdraw your consent.

Don't hesitate to contact us if you wish to exercise the above rights. You will not have to pay a fee to access your PII (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

Where you exercise one of your rights, we may need to request specific information from you to confirm your identity and ensure your right to exercise such rights. This request is a security measure to ensure that PII is not disclosed to anyone with no right to receive it. We may also contact you to ask you for further information about your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is complicated or we are dealing with several of your requests. In this case, we will notify you and update you as we progress.

15. How long is PII retained for before deletion?

PII Generally

We will only retain your PII for as long as necessary to fulfill the purposes we collected it for, including to satisfy any legal, accounting, or reporting requirements.

To determine the appropriate retention period for PII, we consider the amount, nature, and sensitivity of the PII, the potential risk of harm from unauthorized use or disclosure of your PII, the purposes for which we process your PII, and whether we can achieve those purposes through other means, and the applicable legal requirements.

Cloudsmith will usually retain PII for up to seven (7) years following the termination of your account.

By law, we must keep basic information about our customers (including contact, identity, financial, and transaction data) for six years after you cease being a customer for tax purposes. For contract administration, we will also store all data as long as the contract you have placed through us endures and for the six-year limitation period after that in case you raise any claims concerning any products or services you or your employer or another person by whom you have been authorized to use our Services have purchased from us. This section does not apply to Customer Data.

In some circumstances, we may anonymize your PII (so that it can no longer be associated with you) for research or statistical purposes. We may use this information indefinitely without further notice to you.

If you want to cancel your account and initiate your PII deletion, you may do so in your user profile. As above, we will retain and use your information as necessary to comply with our legal obligations, resolve disputes, maintain security, and enforce our agreements. Still, barring legal requirements, the timeframe above will be observed for deletion.

Customer Data

We will endeavor to delete any Customer Data within your packages no later than 12 months after your account is terminated or such Customer Data is deleted using your account; this is to synchronize the deletion of such Customer Data with our annual data deletion cycles and to facilitate the potential provision of a service to you (as our customer) that may permit the restoration of your account, or of accidentally deleted Customer Data, upon request and for payment of a fee. You should note that this is not guaranteed and that Customer Data may be irrevocably deleted more quickly.

16. How does Cloudsmith communicate with users?

We will use your e-mail address to communicate with you if you've said that's okay, and only for the reasons you've indicated. By default, e-mails are not disclosed to other users, even if you belong to the same organization unless you have explicitly revealed them. Your e-mail preferences and disclosure will not change how we contact you, as we always utilize your primary e-mail address.

Depending on your e-mail settings, Cloudsmith may occasionally send notification e-mails about changes in a package repository you're watching, new features, requests for feedback, significant policy changes, or offer customer support. We also send marketing e-mails, but only with your consent. There's an unsubscribe link at the bottom of each of the e-mails we send you.

Our e-mails might contain a pixel tag, a small, clear image that can tell us whether you have opened an e-mail and what your IP address is. We use this pixel tag to make our e-mail more beneficial for you and ensure we're not sending you an unwanted e-mail.

17. Will this privacy policy change?

If there are material changes to this Policy or how we use your PII, we will prominently post such changes before implementing the change. We encourage you to periodically review this Policy to inform us how we collect and use your information.

We keep this Policy under regular review, for example, to reflect changing business circumstances and legal developments.

Although most changes are likely to be minor, they may change, and if it does, they will be posted on this page and, where appropriate, notified to you when you next log on to use our services. Otherwise, any changes shall be applicable without further notice.

18. How can I contact Cloudsmith?

Questions regarding our Privacy Policy or information practices should be directed to us via one of the contact methods we provide.

19. Legal

This Policy shall be governed by and interpreted per the laws of Northern Ireland. You irrevocably agree that Northern Ireland's courts shall have exclusive jurisdiction to settle any that may arise out of, under, or connected with this Policy.

This Policy forms part of our Terms of Service.

If you collaborate on or become a member of an organization/account that has agreed to the Corporate Terms of Service and a Data Protection Addendum (**DPA**) to this Policy, then that DPA governs in the event of any conflicts between this Privacy Statement and the DPA concerning your activity.

APPENDIX 1

Cookies and Other Technologies Policy

1. What specific technical data is collected?

Cloudsmith collects and analyses traffic by keeping track of our visitors' IP addresses and collecting log file information. Your IP address is a number automatically assigned to the computer you are using by your Internet service provider (ISP) or another organization. By itself, an IP address cannot identify you personally unless you are logged in while using our sites. However, when combined with other information, your IP address can be used to determine the computer you are using. Also, Cloudsmith may use your IP address to estimate your geographic location. You may also be personally identifiable from this information where you are logged in when using our services.

The technologies we may use to collect technical data include:

- **Cookies or Browser Cookies.** A cookie is a small file placed on your device that may be used to identify an individual as a unique user by storing specific personal preferences and user data. Cloudsmith uses cookies and other technologies (like HTML5 local storage) to recognize your device, identify authorized users of the Cloudsmith service, track affiliate referrals, complete online purchases through Cloudsmith's billing system, keep you logged in, remember your preferences, provide information for the future development of Cloudsmith and similar undertake website monitoring activities.
- **Web Beacons.** Individual sections of our services, website, and e-mails may also use web beacons, tiny graphic images, or other web programming code (also known as "1x1 GIFs" or "clear GIFs"). Web beacons may be invisible to you, but any electronic image or other web programming code inserted into a web page or e-mail can act as a web beacon. Web beacons or similar technologies may be used for several purposes, including, without limitation, to count visitors to our websites, monitor how users navigate our websites, count how many e-mails that were sent were opened, or count how many particular articles or links were viewed.
- **Embedded Scripts.** These are code designed to collect information about your interactions with a website, such as the links you click on and assist our customers in providing information to deliver our services. The code is temporarily downloaded onto your device from our web server, our customer's web server, or a third-party service provider, is active only while you are connected to our websites containing the embedded script, and is deactivated or deleted after that.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some or all parts of our services. Our services may use cookies unless you have adjusted your browser setting to refuse cookies.

Your web browser automatically sends information to every website you visit, including ours. For example, our server logs may receive and record information such as the pages you access on our websites, referring URLs, your browser type, your operating system, the date and time of your visit, and the duration of your stay on each page.

Log information may also include a user agent string, a series of characters automatically sent with your Internet requests that provide information necessary for smooth Internet communications, such as the operating system and browser you used. Like an IP address, a user agent string does not necessarily identify you personally by itself. However, when combined with other information, a user agent string might identify the computer originating a message.

Cloudsmith may also request access to or otherwise receive information about your device location when you access our websites. Your location data may be based on your IP address. We use location data in connection with providing our services and to help improve our services.

Cloudsmith may assign your computer or mobile device a unique identification number (**Unique ID**) based on log file information when you access our websites. Cloudsmith may set a cookie on your machine containing, amongst other things, the device's Unique ID. Cloudsmith uses data generated from the Unique ID to improve our Services, primarily our ability to detect fraud. Cloudsmith does not share the Unique ID or any associated information with unaffiliated third parties.

Cookies can be “Persistent” or “Session” Cookies. Persistent Cookies remain on your personal computer or mobile device when you go offline, while Session Cookies are deleted as soon as you close your web browser.

Some further examples of the kinds of cookies we use are specified below:

Essential Cookies

Type: Session Cookies

Administered by: Us

Purpose: Essential cookies help make a website usable by enabling basic functions like page navigation, access to secure website areas (via login), or implementing security. The website cannot function properly without these cookies.

Preference Cookies

Type: Persistent Cookies

Administered by: Us and Third-Parties

Purpose: Preference cookies enable a website to remember information that changes how the website or tooling (e.g., Intercom) behaves or looks.

Statistics Cookies

Type: Persistent Cookies

Administered by: Us and Third-Parties

Purpose: Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting usage information. Statistics allow us to understand the service better to focus on improvements.

Marketing Cookies

Type: Persistent Cookies

Administered by: Us and Third-Parties

Purpose: Marketing cookies are used to track visitors across websites. The intention is to display ads (elsewhere) that are relevant and engaging for the individual user or to track which of our ads are successful. We do not show adverts.

Unclassified Cookies

Type: Persistent Cookies

Administered by: Us and Third-Parties

Purpose: Unclassified cookies are cookies that we are in the process of classifying, together with the providers of individual cookies. Being unclassified doesn’t mean they are dangerous or unwanted, just that we have not yet classified them.

2. What specific tracking code or third-party monitoring technologies are used?

Below is a non-exhaustive list of the critical third-party monitoring technologies we use, a brief note of how we use them, what company owns the relevant software packages, and a link to the applicable privacy policies. These links and information are correct and complete to our practical knowledge as this Policy was last revised. Still, you should review the relevant links to ensure you access the most recent and up-to-date version of any policies, for example.

Google Analytics

We use Google Analytics as a third-party tracking service, but we don't use it to track you individually or collect your PII. We use Google Analytics to collect information about how our website performs and how our users, in general, navigate and utilize Cloudsmith; this helps us evaluate our users' use of Cloudsmith; compile statistical reports on activity to improve our content and website performance.

Google Analytics gathers certain simple, non-personally identifying information over time, such as your IP address, browser type, internet service provider, referring and exit pages, time stamp, and similar data about your use of Cloudsmith. We do not link this information to any of your PII, such as your user name.

Cloudsmith will not, nor will we allow any third party to, use the Google Analytics tool to track our users individually, collect any PII other than IP address, or correlate your IP address with your identity. Google provides further information about its privacy practices and offers a browser add-on to opt-out Google Analytics tracking.

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page.

Mixpanel

We use Mixpanel, provided by Mixpanel, Inc., to gather UI application usage metrics. Mixpanel captures specific usage metrics and events to correlate application usage to build a better product. We pay particular attention to not transmitting secretive information (e.g., tokens, passphrases, or passwords) where possible.

You can prevent Mixpanel from using your information for analytics purposes by opting out of analytics.

To opt-out of the Mixpanel service entirely across sites, please visit this page: https://mixpanel.com/optout/.

For more information on what type of Information Mixpanel collects, please visit the Terms of Use page of Mixpanel: https://mixpanel.com/terms/.

HotJar

We use HotJar, provided by HotJar, inc., to gather UI application usage and workflows. HotJar captures specific usage workflows and events to identify workflows' issues and build a better product. We pay particular attention to not transmitting secretive information (e.g., tokens, passphrases, or passwords) where possible.

You can prevent HotJar from using your information for analytics purposes by opting out of analytics.

Their Privacy Policy can be viewed at https://www.hotjar.com/legal/policies/privacy/.

Intercom

We use Intercom as a customer engagement platform. All visitors and users are tracked to associate conversation history with your visit, your account (if logged in), and any Cloudsmith organizations you may belong. Cloudsmith will not share any PII gathered and utilized via Intercom with third-party services.

Their Privacy Policy can be viewed at https://www.intercom.com/legal/privacy.

Tracking

“Do Not Track” is a privacy preference you can set in your browser if you do not want online services to collect and share certain information about your online activity from third-party tracking services. Over time, we do not track your online browsing activity on other online services. We do not permit third-party services to track your activity on our site beyond our basic Google Analytics tracking, from which you may opt-out. Because we do not share this kind of data with third-party services or permit this kind of third-party data collection on Cloudsmith for any of our users, and we do not track our users on third-party websites ourselves, we do not need to respond differently to an individual browser’s Do Not Track setting.

The Do Not Track website has browser-specific instructions if you want to turn on your browser’s privacy and Do Not Track settings.

APPENDIX 2

Our Service Providers

This Appendix sets out a different non-exhaustive list of the critical third-party services providers whose software and services we utilize and with whom your account might otherwise interact, a brief note of how we use them, what company owns the relevant software packages, and a link to the applicable privacy policies for those companies.

These links and information are correct and complete to our practical knowledge as this Policy was last revised. Still, you should review the relevant links to ensure that you access the most recent and up-to-date version of any policies, for example.

1. Third-Party Applications

You have the option of enabling or adding third-party applications to your account. These applications are not necessary for your use of our platform. We will share your PII with third parties when you ask us to; however, you are responsible for using the third-party application and the amount of PII you choose to share with/through it.

E-mail Marketing

We may use your PII in marketing communications, as noted above, and collaborate with e-mail marketing services providers to manage and send e-mails to you. We currently use:

HubSpot

Their Privacy Policy can be viewed at https://legal.hubspot.com/privacy-policy.

Intercom

Their Privacy Policy can be viewed at https://www.intercom.com/legal/privacy.

Payments

We may provide paid and third-party services for payment processing (e.g., payment processors) or payment analytics.

These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express, and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

We currently use:

Stripe (Stripe Inc)

Stripe is a payment service provided by Stripe Inc.

Their Privacy Policy can be viewed at https://stripe.com/us/privacy.

PII collected: various types of Data as specified in the service's privacy policy.

Place of processing: United States.

ChartMogul

Their Privacy Policy can be viewed at https://chartmogul.com/privacy/.

Behavioural Remarketing

We use third-party vendors' remarketing services to advertise on third-party websites to you after visiting our website(s). These third-party vendors collect information about your activity on our website to enable us to:

- Measure and analyze traffic and browsing activity on Our Service
- Show advertisements for our products or services to you on third-party websites
- Measure and analyze the performance of Our advertising campaigns

Some third-party vendors may use non-cookie technologies that may not be impacted by browser settings that block cookies. Your browser may not permit you to stop such technologies. You can use the following third-party tools to decline the collection and use of information to serve you interest-based advertising:

- The NAI's opt-out platform: http://www.networkadvertising.org/choices/
- The EDAA's opt-out platform http://www.youronlinechoices.com/
- The DAA's opt-out platform: http://optout.aboutads.info/?c=2&lang=EN

We may share information, such as hashed e-mail addresses (if available) or other online identifiers collected on our website with these third-party vendors. This identification allows these third-party vendors to recognize and deliver ads to you across devices and browsers. To read more about the technologies used by these third-party vendors and their cross-device capabilities, please refer to the Privacy Policy of each vendor listed below.

The third-party vendors we use for remarketing purposes are:

Google Ads (AdWords)

Google Inc provides the Google Ads (AdWords) advertising service.

You can opt-out of Google Analytics for Display Advertising and customize the Google Display Network ads by visiting the Google Ads Settings page: http://www.google.com/settings/ads

Google also recommends installing the Google Analytics Opt-out Browser Add-on –

https://tools.google.com/dlpage/gaoptout - for your web browser. Google Analytics Opt-out Browser Add-on allows visitors to prevent their data from being collected and used by Google Analytics.

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: https://policies.google.com/privacy.

Bing Ads Remarketing

Microsoft Inc provides Bing Ads advertising service.

You can opt-out of interest-based Bing Ads by following their instructions: https://advertise.bingads.microsoft.com/en-us/resources/policies/personalized-ads.

You can learn more about Microsoft's privacy practices and policies by visiting their Privacy Policy page: https://privacy.microsoft.com/en-us/PrivacyStatement.

Twitter

Twitter Inc provides the Twitter advertising service.

You can opt out of Twitter's interest-based ads by following their instructions: https://support.twitter.com/articles/20170405.

You can learn more about the privacy practices and policies of Twitter by visiting their Privacy Policy page: https://twitter.com/privacy.

AdRoll

NextRoll, Inc provides the AdRoll remarketing service.

You can opt out of AdRoll remarketing by visiting this AdRoll Advertising Preferences web page: http://info.evidon.com/pub_info/573?v=1&nt=1&nw=false or the Opt-Out of Personalized Advertising web page: https://help.adroll.com/hc/en-us/articles/216599538-Opting-Out-of-Personalized-Advertising.

If you are a California resident, please read the "Information For California Residents Only" section in the Privacy Policy of NextRoll, Inc.: https://www.nextroll.com/privacy#service-13.

For more information on the privacy practices of AdRoll, please visit the NextRoll, Inc. Privacy Policy web page: https://www.nextroll.com/privacy.

Hosting & Backend Infrastructure

We use this type of service to host Data and provide the Service. Some parts of these services are geographically distributed, making it difficult to determine where the PII is stored. However, these are still protected by the standard authentication and authorization provided elsewhere.

The third-party vendors we use for hosting & backend infrastructure are:

Amazon Web Services (AWS)

AWS is a market-leading hosting and backend service provided by Amazon.com Inc.

You can learn more about the privacy practices and policies of Amazon Web Services by visiting their Privacy Policy page: https://aws.amazon.com/privacy/.

PII collected: various types of Data as specified in the service's privacy policy.

Place of processing: United States.

Infrastructure Monitoring

We use this service to monitor our Applications and the Service, to detect issues with and measure performance, operation, uptime, maintenance, and usage. The PII that is processed depends upon the implementation of these services and may include log centralization and application usage.

The third-party vendors we use for infrastructure monitoring are:

DataDog

Their Privacy Policy can be viewed at https://www.datadoghq.com/legal/privacy/.

Sentry

Their Privacy Policy can be viewed at https://sentry.io/privacy/.

CloudForecast

Their Privacy Policy can be viewed at https://www.cloudforecast.io/privacy.html.

HotJar

Their Privacy Policy can be viewed at https://www.hotjar.com/legal/policies/privacy/.

Customer Feedback Management

We use this service to manage customer feedback, including feature requests and roadmap insights. The PII processed depends on what the User offers and who provides feedback.

The third-party vendors we use for customer feedback management are:

TypeForm

Their Privacy Policy can be viewed at https://admin.typeform.com/to/dwk6gt/.

Customer Contract Management

We use this type of service to exchange signed contracts with customers. The processed PII must identify an entity that can legally enter into binding contracts.

The third-party vendors we use for customer contract management are:

DocuSign (DocuSign, Inc.)

This service makes it possible for us to manage signed customer contracts. The PII process depends on the user's information while signing the contract.

Their Privacy Policy can be viewed at https://www.docusign.com/company/privacy-policy.

PII collected: e-mail address, first name, last name, billing address.

Place of processing: United States.

Source Code Management

We use this service to manage the source code for the Service.

The third-party vendors we use for source code management are:

GitHub

This service makes it possible to manage source code for the Service. The PII processed depends on the information provided by the User.

Their Privacy Policy can be viewed at https://docs.github.com/en/github/site-policy/github-privacy-statement.

PII collected: various types of Data as specified in the service's privacy policy.

Place of processing: United States.

BitBucket

Their Privacy Policy can be viewed at https://www.atlassian.com/legal/privacy-policy.

Usage, Performance, and Miscellaneous.

Other Services

We also use third-party service providers to better our services. One example is:

reCAPTCHA

An invisible captcha service named reCAPTCHA, operated by Google, Inc.

The reCAPTCHA service may collect information from you and your Device for security purposes.

The information gathered by reCAPTCHA is held per the Privacy Policy of Google: https://www.google.com/intl/en/policies/privacy/.

APPENDIX 3

CCPA Privacy Notice

This privacy notice section for California residents supplements the information contained in our privacy policy. It applies solely to all visitors, users, and others who reside in the State of California, USA, for the California Consumer Privacy Act of 2018 (**CCPA**).

1. Categories of PII collected

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device. The following is a list of PII categories we may have collected from California residents within the last twelve (12) months.

The categories and examples provided in the list below are defined in the CCPA. This definition does not mean that all instances of that category of PII were collected by us but reflects our good-faith belief that some of that information from the relevant category may have been collected. For example, specific PII types would only be collected if you provided such PII directly to us.

Category A: Identifiers.

Examples: A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, e-mail address, account name, driver's license number, passport number, or other similar identifiers.

Collected: Yes.

Category B: Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).

Examples: A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some PII included in this category may overlap with different categories.

Collected: Yes.

Category C: Protected classification characteristics under California or federal law.

Examples: Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth, and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).

Collected: No.

Category D: Commercial Information.

Examples: Records and history of products or services purchased or considered.

Collected: Yes

Category E: Biometric Information.

Examples: Genetic, physiological, behavioral, and biological characteristics or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or different physical patterns, and sleep, health, or exercise data.

Collected: No.

Category F: Internet or other similar network activity.

Examples: Interaction with our services or advertisement.

Collected: Yes.

Category G: Geolocation data.

Examples: Approximate physical location.

Collected: Yes.

Category H: Sensory data.

Examples: Audio, electronic, visual, thermal, olfactory, or similar information.

Collected: No.

Category I: Professional or employment-related information.

Examples: Current or past job history or performance evaluations.

Collected: No.

Category J: Non-public education information (per the Family Educational Rights and Privacy Act (20 USC Section 1232g, 34 CFR Part 99)).

Examples: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.

Collected: No.

Category K: Inferences drawn from other personal information.

Examples: Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Collected: No.

Exclusions

Under CCPA, personal information does not include:

Publicly available information from government records;

Deidentified or aggregated consumer information;

Information excluded from the CCPA's scope, such as:

Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data

Specific sector-specific privacy laws cover personal information, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

2. Sources of personal information

We obtain the categories of personal information listed above from the following types of sources:

Directly from You. For example, from the forms you complete on our Service, preferences you express or provide through our Service, or from your purchases on our Service.

Indirectly from You. For example, from observing your activity on our Service.

Automatically from You. For example, we or our service providers set on your device as you navigate our Service through cookies.

From Service Providers. For example, third-party vendors to monitor and analyze our Service, third-party vendors to deliver targeted advertising to You, third-party vendors for payment processing, or other third-party vendors we use to provide your services.

USE OF PERSONAL INFORMATION FOR BUSINESS PURPOSES OR COMMERCIAL PURPOSES

We may use or disclose personal information we collect for "business purposes" or "commercial purposes" (as defined under the CCPA), as further set out in the "How Is Your Information Used" in the main section of our Policy above.

If we decide to collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes, we will update this Policy.

DISCLOSURE OF PERSONAL INFORMATION FOR BUSINESS PURPOSES OR COMMERCIAL PURPOSES

We may use or disclose and may have used or disclosed in the last twelve (12) months the following categories of personal information for business or commercial purposes:

Category A: Identifiers

Category B: Personal Information listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))

Category D: Commercial Information

Category F: Internet or other similar network activity

Please note that the categories listed above are those defined in the CCPA; this does not mean that all examples of that category of PII were disclosed but reflects our good-faith belief, to the best of our knowledge, that some of that information from the relevant category may be and may have been disclosed.

When we disclose PII for a business purpose or a commercial purpose (other than to a regulatory or government body or to other users with whom any user's account is affiliated), we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

3. Sale of personal information

As defined in the CCPA, “sell” and “sale” mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for valuable consideration. We do not sell personally-identifying information.

4. Sharing of personal information

We may share your PII identified in the above categories with the categories of third parties identified in the “What Information is Shared?” section above.

5. Your rights under the CCPA

The CCPA provides California residents with specific rights regarding their personal information. If you are a resident of California, you have the following rights:

The right to notice. You have the right to be notified of which categories of PII are being collected and the purposes for which the PII is being used.

The right to request. Under CCPA, you have the right to request that we disclose information to you about Our collection, use, sale, disclosure for business purposes, and share of personal information. Once we receive and confirm your request, we will disclose to you:

The categories of personal information we collected about You;

The categories of sources for the personal information we collected about You;

Our business or commercial purpose for collecting or selling that personal information;

The categories of third parties with whom we share that personal information; and

The specific pieces of personal information we collected about You.

The right to delete PII. You have the right to request the deletion of your PII, subject to certain exceptions. Once we receive and confirm your request, we will delete (and direct our services providers to delete) your personal information from our records unless an exception applies. We may deny your deletion request if retaining the data is necessary for our service providers or us to:

Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with You;

Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such actions;

Debug products to identify and repair errors that impair existing intended functionality;

Exercise free speech, ensure the right of another consumer to exercise their free speech rights or exercise another right provided for by law;

Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.);

Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the information’s deletion may likely render impossible or seriously impair the research’s achievement if you previously provided informed consent;

Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with Us;

Comply with a legal obligation; and

Make other internal and lawful uses of that information compatible with the context in which you provided it.

The right not to be discriminated against. You have the right not to be discriminated against for exercising any of your consumer's rights, including by us:

Denying goods or services to you;

Charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties;

Providing a different level or quality of goods or services to you; and

Suggesting that you will receive a different price or rate for goods or services or a different level or quality of goods or services.

6. Exercising your CCPA data protection rights

To exercise your rights under the CCPA, you can contact us using the contact methods specified above if you are a California resident.

Only you, or a person registered with the California Secretary of State you authorize to act on your behalf, may make a verifiable request related to your personal information.

Your request to us must:

Provide sufficient information that allows us to reasonably verify that you are the person about whom we collected personal information or an authorized representative

Describe your request with sufficient detail that will enable us to understand, evaluate, and respond to it properly

We cannot respond to your request or provide you with the required information if we cannot:

Verify your identity or authority to make the request; and

Confirm that the personal information relates to you.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is complicated or there are several of them. In this case, we will notify you and keep you updated.

Any disclosures we provide will only cover the 12 months preceding the verifiable request's receipt. For data portability requests, we will select a format to provide your personal information that is readily usable and allow you to transmit the information from one entity to another without hindrance.

7. Do not sell my personal information

While Cloudsmith does not sell information, our services providers (for example, our analytics or advertising partners) may use technology on our services that sell personal information as defined by the CCPA. Suppose you wish to opt-out of using your data for interest-based advertising purposes and these potential sales as described under the CCPA. In that case, you may do so by following the instructions below.

Please note that any opt-out is specific to the browser you use. You may need to opt-out of every browser that you use.

8. Website

You can opt-out of receiving ads that are personalized as served by our service providers by following the instructions presented on our services:

The NAI's opt-out platform: http://www.networkadvertising.org/choices/

The EDAA's opt-out platform http://www.youronlinechoices.com/

The DAA's opt-out platform: http://optout.aboutads.info/?c=2&lang=EN

The opt-out will place a cookie on your computer unique to the browser you use to opt-out. If you change browsers or delete the cookies saved by your browser, you will need to opt-out again.

9. Mobile devices

Your mobile device may give you the ability to opt-out of the use of information about the apps you use to serve you ads that are targeted to your interests:

“Opt-out of Interest-Based Ads” or “Opt-out of Ads Personalization” on Android devices.

“Limit Ad Tracking” on iOS devices.

You can also stop collecting location information from your mobile device by changing your device’s preferences.

10. Do not track

“Do Not Track” Policy as Required by California Online Privacy Protection Act (CalOPPA)

Our services do not respond to Do Not Track signals. However, some third-party websites do keep track of your browsing activities. If you visit such websites, you can set your web browser preferences to inform websites to disable such tracking. You can enable or disable DNT by visiting your web browser’s preferences or settings page.

11. Your California privacy rights (California’s Shine The Light Law)

Under California Civil Code Section 1798 (California’s Shine the Light law), California residents with an established business relationship with us can request information once a year about sharing their Data with third parties for the third parties’ direct marketing purposes.

If you’d like to request more information under the California Shine the Light law, and if you are a California resident, you can contact us using the contact information provided below.

CALIFORNIA PRIVACY RIGHTS FOR MINOR USERS (CALIFORNIA BUSINESS AND PROFESSIONS CODE SECTION 22581)

California Business and Professions Code section 22581 allows California residents under the age of 18 who are registered users of online sites, services, or applications to request and obtain the removal of content or information they have publicly posted.

To request the removal of such data, and if you are a California resident, you can contact us using the contact information provided below and include the e-mail address associated with your account.

Be aware that your request does not guarantee complete or comprehensive removal of content or information posted online and that the law may not permit or require removal in certain circumstances.