

Privacy Policy

Effective Date: [August 8th, 2025]

1.Introduction

This is a Privacy Policy of Opus Inc. (“Opus”, “we”, “us”) , with its legal address at 580 California St., Suite 1205, SF, CA 94104, United States of America. Opus provides AI clipping and editing platform, turning videos into shorts. This Privacy Policy explains how we process personal data of individuals who use our services, including our platform, websites (e.g. opus.pro), and other product and Services (“Services”).

At Opus, we take your privacy seriously. Please read this Privacy Policy to learn how we treat your personal data. By using or accessing our Services in any manner, you acknowledge that you accept the practices and policies outlined below, and you hereby consent that we will collect, use and share your information as described in this Privacy Policy.

Remember that your use of Opus' Services is at all times subject to our [Terms of Services](#), which incorporates this Privacy Policy. Any terms we use in this Policy without defining them have the definitions given to them in the Terms of Services.

This Policy applies where we offer our Services, products, and platforms to individual users. For purposes of this Privacy Policy, Opus is usually the processor of your personal data. We are the controller only if we process data for our own legitimate purposes.

You may print a copy of this Privacy Policy by clicking [here](#).

Opus complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Opus has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF

Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Opus has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program and to view our certification, please visit <https://www.dataprivacyframework.gov/>. Opus is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). As we continually work to improve our Services, we may need to change this Privacy Policy from time to time. Upon such changes, we will alert you to any such changes by placing a notice on the Opus website, by sending you an email and/or by some other means. Please note that if you've opted not to receive legal notice emails from us (or you haven't provided us with your email address), those legal notices will still govern your use of the Services, and you are still responsible for reading and understanding them. If you use the Services after any changes to the Privacy Policy have been posted, that means you agree to all of the changes.

2.Scope – What Does This Policy Cover?

This Privacy Policy covers how we process treat Personal Data that we gather when you access or use our Services. "Personal Data" means any information relating to an identified or identifiable individual, such as e.g. an individual's name, address, telephone number, or email address. means any information that identifies or relates to a particular individual and also includes information referred to as "personally identifiable information" or "personal information" under applicable data privacy laws, rules or regulations. This Privacy Policy

does not cover the practices of companies we don't own or control or people we don't manage.

3.What Information Do We Collect, and for What Purposes?

Categories of Personal Data We Collect, Purposes and Legal Basis for Processing according to the GDPR

For your convenience, this chart details the categories of Personal Data that we collect and have collected over the past 12 months:

Category of Personal Data and examples	Purpose and Legal Basis for Processing Based on the GDPR	Categories of Third Parties with Whom We Share this Personal Data
Profile or Contact Data: <ul style="list-style-type: none">• First and last name• Email• Phone number	Purpose: Account creation, authentication, customer support Legal Basis: Contractual necessity	<ul style="list-style-type: none">• Service provider• Advertising partners• Analytics partners• Business partners• Parties You Authorize, Access, or Authenticate
Commercial Data: <ul style="list-style-type: none">• Purchase history	Purpose: Maintain logs to detect bugs, security incidents, and deliver the service Legal Basis: Contractual necessity and legitimate interest	<ul style="list-style-type: none">• Parties You Authorize, Access, or Authenticate• Service Providers
Device/IP Data: <ul style="list-style-type: none">• IP address• Device ID• Type of device/operating system/browser used to access the Services• Device fingerprint	Purpose: Service security, troubleshooting, analytics Legal Basis: Legitimate interest	<ul style="list-style-type: none">• Advertising Partners• Analytics Partners• Service Providers

<p>Web analytics:</p> <ul style="list-style-type: none"> • Web page interactions • Referring webpage/source through which you accessed the Services • Non-identifiable request IDs • Statistics associated with the interaction between devices or browser and the Services • Browsing or search history 	<p>Purpose: Remember settings, measure reach, show ads</p> <p>Legal Basis: Consent (except for essential cookies) and legitimate interest</p>	<ul style="list-style-type: none"> • Advertising Partners • Analytics Partners • Parties You Authorize, Access or Authenticate • Service Providers
<p>Social Network Data:</p> <ul style="list-style-type: none"> • Email • User name • Information from User's social media profile (public data may include users' videos posted publicly on their social media accounts and any associated statistics; authorized access to private data may include internal performance analytics of social media profiles) 	<p>Purpose: Provide the integration the user requested (e.g. import videos, publish clips), show social-media performance metrics in dashboard, improve creator-tool features & benchmark trends</p> <p>Legal Basis: Contractual necessity and consent</p>	<ul style="list-style-type: none"> • Service Providers • Analytics Partners • Parties You Authorize, Access or Authenticate
<p>Geolocation Data:</p> <ul style="list-style-type: none"> • IP address-based location information • Browser time zone 	<p>Purpose: Detect suspicious log-ins and payment fraud</p> <p>Legal Basis: Legitimate interest</p>	<ul style="list-style-type: none"> • Service Providers • Advertising Partners • Analytics Partners

<p>Inferences Drawn from Other Personal Data Collected:</p> <ul style="list-style-type: none"> • Inferences reflecting user attributes • Inferences reflecting user behavior • Inferences reflecting user preferences or abilities/aptitudes 	<p>Purpose: Personalizing services</p> <p>Legal Basis: Contractual necessity</p>	<ul style="list-style-type: none"> • Service Providers • Advertising Partners • Analytics Partners
<p>User-generated content:</p> <ul style="list-style-type: none"> • videos, images, transcripts 	<p>Purpose: Provide editing & sharing features, improve product and services</p> <p>Legal Basis: Contractual necessity, legitimate interest</p>	<ul style="list-style-type: none"> • Service Providers • Advertising Partners • Analytics Partners
<p>Information you provide to us. Depending upon the context in which you interact with us, personal information you may provide to us through the Service includes: text, images, video, PDFs, scripts, audio (including data to clone your voice), URLs, prompts, and other assets.</p>	<p>Purpose:</p> <ul style="list-style-type: none"> • understand your needs and interests; • personalize your experience with the Service and our Service-related communications; • remember your selections and preferences as you navigate webpages. <p>Legal Basis: Legitimate Interest</p>	<ul style="list-style-type: none"> • Service Providers • Advertising Partners • Analytics Partners

Special Categories of Personal Data (Art 9 GDPR)

Opus does not request, collect, or intentionally process any “special categories of personal data” within the meaning of Article 9 GDPR — that is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data for uniquely identifying a person, health information, or data concerning a person’s sex life or sexual orientation. We ask that you do not upload or

otherwise share such information when you use the Services. Opus does not collect Sensitive Personal Data, as such term is defined under U.S. State Privacy Laws.

Payment data

When you purchase a subscription or pay for any Opus service, your payment data (card type, last 4 digits, expiry month/year, billing name, address, e-mail and transaction identifiers) are collected and processed by Stripe. Your payment data are handled in line with Stripe's own privacy policy, which you can review at <https://stripe.com/privacy>.

Categories of Sources of Personal Data

We collect Personal Data about you from the following categories of sources:

- **You**
 - When you provide such information directly to us.
 - When you create an account or use our interactive tools and Services.
 - When you voluntarily provide information in free-form text boxes through the Services or through responses to surveys or questionnaires.
 - When you send us an email or otherwise contact us.
 - When you use the Services and such information is collected automatically.
 - Through Cookies (defined in the "Tracking Tools, Advertising and Opt-Out" section below).
 - If you download our mobile application or use a location-enabled browser, we may receive information about your location and mobile device, as applicable.
 - If you download and install certain applications and software we make available, we may receive and collect information transmitted from your computing device for the purpose of providing you the relevant Services, such as information regarding when you are logged on and available to receive updates or alert notices.
- **Public Records**

- From the government or other sources.
- **Third Parties**
 - Vendors
 - We may use analytics providers to analyze how you interact and engage with the Services, or third parties may help us provide you with customer support.
 - We may use vendors to obtain information to generate leads and create user profiles.
 - Advertising Partners
 - We receive information about you from some of our vendors who assist us with marketing or promotional services related to how you interact with our websites, applications, products, Services, advertisements or communications.
 - Social Networks
 - If you provide your social network account credentials to us or otherwise sign in to the Services through a third-party site or service, some content and/or information in those accounts may be transmitted into your account with us.

Our Commercial or Business Purposes for Collecting or Disclosing Personal Data

Providing, Customizing and Improving the Services

- Creating and managing your account or other user profiles.
- Processing orders or other transactions; billing.
- Providing you with the products, services or information you request.
- Meeting or fulfilling the reason you provided the information to us.
- Providing support and assistance for the Services.
- Improving the Services, including testing, research, internal analytics and product development.
- Personalizing the Services, website content and communications based on your preferences.
- Doing fraud protection, security and debugging.

Carrying out other business purposes stated when collecting your Personal Data or as otherwise set forth in applicable data privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the “CCPA”) the Colorado Privacy Act (the “CPA”), the Connecticut Data Privacy Act (the “CTDPA”), Delaware Personal Data Privacy Act (“DPDPA”), Iowa Consumer Data Protection Act (“ICDPA”), Montana Consumer Data Privacy Act (“MCDPA”), Nebraska Data Privacy Act (“NDPA”), Oregon Consumer Privacy Act (“OCPA”), the Texas Data Privacy and Security, Act (“TDPSA”), New Hampshire Privacy Act (“NHPA”), New Jersey Privacy Act (“NJPA”), Utah Consumer Privacy Act (the “UCPA”), or the Virginia Consumer Data Protection Act (the “VCDPA”) (collectively, the “U.S. State Privacy Laws”).

Marketing the Services

- Marketing and selling the Services.
- Showing you advertisements, including interest-based or online behavioral advertising.

Corresponding with You

- Responding to correspondence that we receive from you, contacting you when necessary or requested, and sending you information about Opus or the Services.
- Sending emails and other communications according to your preferences or that display content that we think will interest you.

Meeting Legal Requirements and Enforcing Legal Terms

- Fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal or prohibited activities.
- Protecting the rights, property or safety of you, Opus or another party.
- Enforcing any agreements with you.
- Responding to claims that any posting or other content violates third-party rights.
- Resolving disputes.

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated or incompatible purposes without providing you notice.

If you are a California resident, please note that we only use or disclose your sensitive personal information for the purposes set forth in section 7027(m) of the CCPA regulations and we do not collect or process sensitive personal information with the purpose of inferring any characteristics about California residents.

5. How Do We Share Your Data?

How We Disclose Your Personal Data

We disclose your Personal Data to the categories of service providers and other parties listed in this section. Depending on laws or regulations that may be applicable to you, some of these disclosures may constitute a “sale” of your Personal Data. For more information, please refer to the state-specific sections below.

- **Service Providers.** These parties help us provide the Services or perform business functions on our behalf. They include:
 - Hosting, technology and communication providers.
 - Analytics providers.
 - Support and customer service vendors.
 - Payment processors.
 - ◆ Our payment processing partner Stripe, Inc. (“Stripe”) collects your voluntarily-provided payment card information necessary to process your payment.
 - ◆ Please see Stripe’s terms of service and privacy policy for information on its use and storage of your Personal Data.
- **Advertising Partners.** These parties help us market our services and provide you with other offers that may be of interest to you. They include:
 - Ad networks.
 - Marketing providers.

- **Analytics Partners.** These parties provide analytics on web traffic or usage of the Services. They include:
 - Companies that track how users found or were referred to the Services.
 - Companies that track how users interact with the Services.
- **Business Partners.** These parties partner with us in offering various services. They include:
 - Businesses that you have a relationship with.
 - Companies that offer marketing tools (e.g., social media scheduling tools) and creator tools integrated with our products.
 - Companies that we partner with to offer joint promotional offers or opportunities.
- **Parties You Authorize, Access or Authenticate**
 - Third parties you access through the services.
 - Social media services.

Legal Obligations

We may share any Personal Data that we collect with third parties in conjunction with any of the activities set forth under “Meeting Legal Requirements and Enforcing Legal Terms” in the “Our Commercial or Business Purposes for Collecting Personal Data” section above.

Business Transfers

All of your Personal Data that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices. In such case an appropriate joint-controllership or data protection agreements will be entered into, to ensure an appropriate level of data protection.

6.Cookies and Other Tracking Technologies

The Services use cookies and similar technologies such as pixel tags, web beacons, clear GIFs and JavaScript (collectively, “Cookies”) to enable our servers to recognize your web browser, tell us how and when you visit and use our Services, analyze trends, learn about our user base and operate and improve our Services. Cookies are small pieces of data– usually text files – placed on your computer, tablet, phone or similar device when you use that device to access our Services. We may also supplement the information we collect from you with information received from third parties, including third parties that have placed their own Cookies on your device(s). Please note that because of our use of Cookies, the Services do not support “Do Not Track” requests sent from a browser at this time.

We use the following types of Cookies:

- Essential Cookies. Essential Cookies are required for providing you with features or services that you have requested. For example, certain Cookies enable you to log into secure areas of our Services. Disabling these Cookies may make certain features and services unavailable.
- Functional Cookies. Functional Cookies are used to record your choices and settings regarding our Services, maintain your preferences over time and recognize you when you return to our Services. These Cookies help us to personalize our content for you, greet you by name and remember your preferences (for example, your choice of language or region).
- Performance/Analytical Cookies. Performance/Analytical Cookies allow us to understand how visitors use our Services. They do this by collecting information about the number of visitors to the Services, what pages visitors view on our Services and how long visitors are viewing pages on the Services. Performance/Analytical Cookies also help us measure the performance of our advertising campaigns in order to help us improve our campaigns and the Services’ content for those who engage with our advertising. For example, Google LLC (“Google”) uses cookies in

connection with its Google Analytics services. Google's ability to use and share information collected by Google Analytics about your visits to the Services is subject to the Google Analytics Terms of Services and the Google Privacy Policy. You have the option to opt-out of Google's use of Cookies by visiting the Google advertising opt-out page at www.google.com/privacy_ads.html or the Google Analytics Opt-out Browser Add-on at <https://tools.google.com/dlpage/gaoptout/>.

- Retargeting/Advertising Cookies. Retargeting/Advertising Cookies collect data about your online activity and identify your interests so that we can provide advertising that we believe is relevant to you. For more information about this, please see the section below titled "Information about Interest-Based Advertisements."
- You can decide whether or not to accept Cookies through your internet browser's settings. Most browsers have an option for turning off the Cookie feature, which will prevent your browser from accepting new Cookies, as well as (depending on the sophistication of your browser software) allow you to decide on acceptance of each new Cookie in a variety of ways. You can also delete all Cookies that are already on your device. If you do this, however, you may have to manually adjust some preferences every time you visit our website and some of the Services and functionalities may not work.
- To explore what Cookie settings are available to you or to modify your preferences with respect to Cookies, you can access your Cookie management settings by clicking <LINK>. To find out more information about Cookies generally, including information about how to manage and delete Cookies, please visit <http://www.allaboutcookies.org/> or <https://ico.org.uk/for-the-public/online/cookies/> if you are located in the European Union.

Information about Interest-Based Advertisements:

We may serve advertisements, and also allow third-party ad networks, including third-party ad servers, ad agencies, ad technology vendors and research firms, to serve advertisements through the Services. These

advertisements may be targeted to users who fit certain general profile categories or display certain preferences or behaviors (“Interest-Based Ads”). Information for Interest-Based Ads (including Personal Data) may be provided to us by you, or derived from the usage patterns of particular users on the Services and/or services of third parties. Such information may be gathered through tracking users’ activities across time and unaffiliated properties, including when you leave the Services. To accomplish this, we or our service providers may deliver Cookies, including a file (known as a “web beacon”) from an ad network to you through the Services. Web beacons allow ad networks to provide anonymized, aggregated auditing, research and reporting for us and for advertisers. Web beacons also enable ad networks to serve targeted advertisements to you when you visit other websites. Web beacons allow ad networks to view, edit or set their own Cookies on your browser, just as if you had requested a web page from their site.

Users in the European Union should visit the European Interactive Digital Advertising Alliance’s user information website

<http://www.youronlinechoices.eu/>.

7.How Long Do We Store Your Information?

We retain Personal Data about you for as long as necessary to provide you with our Services or to perform our business or commercial purposes for collecting your Personal Data. When establishing a retention period for specific categories of data, we consider who we collected the data from, our need for the Personal Data, why we collected the Personal Data, and the sensitivity of the Personal Data. In some cases we retain Personal Data for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

For example:

- We retain your profile information and credentials for as long as you have an account with us.
- We retain your payment data for as long as we need to process your purchase or subscription.
- We retain your device/IP data for as long as we need it to ensure that our systems are working appropriately, effectively and efficiently.

8.How Do We Secure Your Information?

Data security is of great importance to us, and to protect your personal information, we have put in place suitable technical, organizational, physical, electronic, and managerial procedures designed to safeguard and secure personal information collected through our Site. You can review them here (<https://trust.opus.pro/>) We seek to protect your Personal Data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of Personal Data and how we are processing that data.

Notwithstanding any security measures that we take, it is important to remember that the transmission of data via the Internet may not be completely secure, and we cannot guarantee that the collection, transmission and storage of data will always be secure. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure. Please take suitable precautions when transmitting data via the Internet to us.

You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism; limiting access to your computer or device and browser; and signing off after you have finished accessing your account. Although we work to protect the security of your

account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure. For the details about our security measures, please visit our Trust Portal: <https://trust.opus.pro/>.

9.Children's Privacy

As noted in the Terms of Services, we do not knowingly collect or solicit Personal Data about children under 16 years of age. If you are a child under the age of 16, please do not attempt to register for or otherwise use the Services or send us any Personal Data. If we learn we have collected Personal Data from a child under 16 years of age, we will delete that information as quickly as possible. If you believe that a child under 16 years of age may have provided Personal Data to us, please contact us at account.deletion@opus.pro.

10.Subprocessors and Third-Party Websites And Materials

We are not responsible for the privacy or security of, information found on, or any practices employed by any third-party applications, websites, or services linked to or from our Service. Although we may provide links to third-party websites or platforms, or display content, data, applications or materials from third parties, our Privacy Policy does not apply to those third-party sites or materials, and your browsing and interaction on any third-party site, application, or service, including those that have a link on our Services, are subject to that third party's own terms and policies.

The current list of sub-processors can be found here. We reserve the right to engage new sub-processors, provided that they meet a high level of security and data protection. We enter into Data Protection Agreements with all of our sub-processors.

11. Additional U.S. State Disclosures and Rights

U.S. State Privacy Rights

If you reside in certain U.S. states such as California, Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia you may have certain rights afforded to you (as described below) depending on your state of residence. Please see the 'Exercising Your Rights under U.S. State Privacy Laws' section below for instructions regarding how to exercise these rights. Please note that we may process Personal Data of our customers' end users or employees in connection with our provision of certain services to our customers. If we are processing your Personal Data as a service provider, you should contact the entity that collected your Personal Data in the first instance to address your rights with respect to such data. Please note that your rights may be subject to certain conditions or exceptions in accordance applicable U.S. State Privacy Laws.

If you have any questions about this section or whether any of the following rights apply to you, please contact us at contact@opus.pro.

-
- Access: You may have the right to request confirmation of or access to the Personal Data that we process about you. You can also request access to a portable copy of your Personal Data. If you are an Oregon resident, you also have the right to request a list of specific third parties, other than natural persons, to which we have disclosed your Personal Data.
- Deletion: You may have the right to request that we delete the Personal Data that we have collected about you.
- Correction: You may have the right to request that we correct any inaccurate Personal Data we have collected about you.

- Portability: You may have the right to request a copy of your Personal Data in a machine-readable format, to the extent technically feasible.

“Selling,” “Sharing,” or “Targeted Advertising”

Depending on your state of residence, you may have the right to opt out from the “sale,” “share,” or disclosure of your Personal Data for the purposes of targeted advertising. These or similar terms may be defined differently depending the applicable U.S. State Privacy Law.

You have the right to opt-out of the sale or share of your Personal Data by following the instructions in the “Exercising Your Rights under U.S. State Privacy Laws” section. Once you have submitted an opt-out request, we will not ask you to reauthorize the sale of your Personal Data for at least 12 months.

As described in the “Tracking Tools, Advertising and Opt-Out” section above, Certain Cookies placed by third parties into our Services may allow those third parties to collect your Personal Data for targeted advertising purposes. Under certain U.S. State Privacy Laws, this may also constitute a “sale” and/or “share” of your Personal Data. For clarity, when we use the term “sell,” we mean for valuable consideration and not for any monetary value.

We sell or share your Personal Data to the following categories of third parties:

Advertising Partners

Over the past 12 months, we have sold or shared the following categories of your Personal Data to categories of third parties listed above:

- Profile or Contact Data
- Device/IP Data
- Web Analytics
- Geolocation Data

We have sold or shared the foregoing categories of Personal Data for the following business or commercial purposes:

- Marketing and selling the Services.

- Showing you advertisements, including interest-based or online behavioral advertising.
- To our knowledge, we do not sell or share the Personal Data of minors under 18 years of age.

Anti-Discrimination

We will not discriminate against you for exercising your rights under applicable privacy laws. We will not deny you our goods or services, charge you different prices or rates, or provide you a lower quality of goods and services if you exercise your rights under applicable privacy laws. However, we may offer different tiers of our Services as allowed by applicable data privacy laws with varying prices, rates or levels of quality of the goods or services you receive related to the value of Personal Data that we receive from you.

Other State-Specific Privacy Rights

Under California Civil Code Sections 1798.83-1798.84, California residents are entitled to contact us to prevent disclosure of Personal Data to third parties for such third parties' direct marketing purposes; in order to submit such a request, please contact us at contact@opus.pro.

Your browser may offer you a "Do Not Track" option, which allows you to signal to operators of websites and web applications and services that you do not wish such operators to track certain of your online activities over time and across different websites. Our Services do not support Do Not Track requests at this time. To find out more about "Do Not Track," you can visit www.allaboutdnt.com.

If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties. Please note that we do not currently sell your Personal Data as sales are defined in Nevada Revised Statutes Chapter 603A.

Exercising Your Rights under U.S. State Privacy Laws

To exercise the rights described in this Privacy Policy, you or your Authorized Agent (if applicable and as defined below), must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected Personal Data (such as your Contact or Profile Data), and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a "Valid Request." We may not respond to requests that do not meet these criteria. We will only use Personal Data provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within the time period required by applicable privacy laws. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

Request to Opt-Out of Sale, Share, and/or Targeted Advertising

As applicable, you may opt-out from any "sales," "shares," or targeted advertising through Cookies, by using the following methods:

- By accessing your cookie consent mechanism by accessing your "Cookie Settings" at the bottom left of our website.
- By implementing the Global Privacy Control or similar universal privacy control that is legally recognized by a government agency or industry standard and that complies with applicable State Privacy Laws. The signal issued by the control must be initiated by your browser and applies to the specific device and browser you use at the time you cast the signal.

Please note this does not include Do Not Track signals.

Request to Access, Delete, Correct

As applicable, you may submit a Valid Request for your right to access, delete, correct, or obtain a copy of your Personal Data described in this Privacy Policy by using the following methods:

- Email us at: contact@opus.pro

- If you are a California, Colorado, Connecticut, Delaware, Montana, Nebraska, New Hampshire, New Jersey Oregon, or Texas resident, you may also authorize an agent (an “Authorized Agent”) to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf.

Appealing a Denial

If you are a Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, or Virginia resident and we refuse to take action on your request within a reasonable period of time after receiving your request in accordance with this section, you may appeal our decision. In such appeal, you must (1) provide sufficient information to allow us to verify that you are the person about whom the original request pertains and to identify the original request, and (2) provide a description of the basis of your appeal. Please note that your appeal will be subject to your rights and obligations afforded to you under the State Privacy Laws (as applicable). We will respond to your appeal within the time period required under the applicable law. You can submit a Verified Request to appeal by the following methods:

- Email us at: contact@opus.pro (subject line must include “[STATE OF RESIDENCE] Appeal”)
- If we deny your appeal, you have the right to contact the Attorney General of your State, including by the following links: [Colorado](#), [Connecticut](#), [Delaware](#), [Iowa](#), [Montana](#), [Nebraska](#), [New Hampshire](#), [New Jersey](#), [Oregon](#), [Texas](#), and [Virginia](#).

12.International Data Transfers

Opus runs on secure Google Cloud servers located in the United States. By using our Services, you understand that your personal information may be

processed and stored on servers, and transferred to third parties, outside your country of residence, including the United States.

If you normally reside in the European Region, the personal data that we collect from you will be further transferred to, and stored at, a destination outside of the EEA (for instance, to our service providers and partners). These transfers are made pursuant to appropriate safeguards, such as standard data protection clauses adopted by the European Commission.

The personal information that you provide to us and that we collect from you will be transferred to, stored at, or processed in, countries outside your country of residence, such as to the United States. Your personal information is also processed by staff operating outside the EEA, UK or Switzerland who work for us or one of our third-party service providers or partners. We process the personal information that you provide to us in countries outside your country of residence in order to provide our Services, perform our contract with you, and provide our website's functionality.

We also use standard contractual clauses (SCCs) as relevant for certain transfers of personal information to third countries, unless the transfer is to a country that has been determined to provide an adequate level of protection for individuals' rights and freedoms for their personal information.

We require that third parties to whom we transfer personal data comply with the Data Privacy Framework principles. We use standard contractual clauses (SCCs) to ensure adequate protection for personal data transferred outside the EU, UK, and Switzerland.

Pursuant to the DPF Program, EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under the DPF, should direct their query to contact@opus.pro. If requested to remove data, we will respond within a reasonable timeframe.

Moreover, in accordance with the DPF Principles, we provide you with the choice to opt out of the disclosure of your personal information to a third party or its use for a purpose that is materially different from the purpose for which it was originally collected. You can exercise this right by contacting us at contact@opus.pro or managing your cookie preferences.

13. Data Rights of International Users

If you are a user located outside of the United States, the following terms apply. Our goal is to provide all our international users with a consistent and high standard of data protection.

Regardless of your location, we recognize a set of data privacy rights. If you have questions about these rights or need to exercise them, you can contact us at contact@opus.pro. We will respond to your request within the timeframe required by applicable law, and we may need to verify your identity before processing your request.

Your rights include:

Right	What it means in practice
Access	Get confirmation that we process your data and receive a copy of the data we hold about you.
Rectification	Have incomplete or inaccurate data we hold about you corrected.
Erasure	Ask us to delete your personal data where it is no longer needed, you withdraw consent, or there is no overriding legal basis to retain it.
Restriction	Ask us to temporarily stop processing your data (but continue to store it) while we resolve a separate request from you.
Data Portability	Receive the data you provided to us in a structured, machine-readable format or ask us to transmit it to another service.

Objection	Object to our processing of your data for direct marketing or when we base the processing on our legitimate interests.
Withdraw Consent	If we process data based on your consent, you may withdraw it at any time. This will not affect the lawfulness of processing done before your withdrawal.
Lodge a Complaint	You have the right to lodge a complaint with the applicable data protection authority about our collection and use of your Personal Data.

Opt-Out & Right to Object to AI Research and Development

If you are based in the European Union or European Economic Area, you are free to opt out of any use of your personal data for our AI research and model-development activities. Under Article 21 GDPR, you may object at any time to such processing. Send an e-mail to contact@opus.pro with the subject line “AI R&D – Opt-Out” and tell us the identifier (e.g., account e-mail or customer number) under which we hold your data and we will opt your data out of this processing.

Automated Decision Making and Profiling

Depending on the state or country of your residence, you may have the right to opt-out the use of automated decision making technology or from the processing of your Personal Data for the purposes of profiling in furtherance of decisions that produce legal or similarly significant effects to you, if applicable. However, we do not process your Personal Data in this manner.

All Other Data Deletion Rights

If you use our services in other jurisdictions or on platforms that grant you the right to request deletion of your data, please send an email to exercise that right at: account.deletion@opus.pro

14. Additional Jurisdiction-Specific Terms

For users in the following jurisdictions, these additional terms apply.

Age and Parental Consent Requirements

Certain jurisdictions have specific age requirements for using our Services.

- Brazil: If you are between 16 and 18, you may only use the Services with the assistance of a parent or legal guardian. If you are under 16, you must be represented by a parent or legal guardian who provides consent.
- Egypt, South Africa: You must be over the age of 18 or have your parent or legal guardian agree to this Policy on your behalf.
- Indonesia: You must be at least 21 years of age, married, or not under guardianship. Otherwise, your parent or legal guardian must provide approval and be responsible for your use of the Services.
- Mexico: If you are under 18 years of age, you may exercise your data rights through a parent or guardian.
- South Korea: The Services are not directed at children under the age of 14.
- Vietnam: You must be at least 16 years of age or have the approval of a parent or legal guardian.

Country-Specific Provisions

- Brazil: In certain situations, we may have legitimate reasons not to comply with a data rights request, for instance, to protect our trade secrets or to comply with a legal obligation. We will inform you of the reason if we cannot fulfill your request.
- Indonesia: In the event of a data breach, we will notify you in accordance with applicable law. We retain data for five (5) years or longer if necessary for legal claims.

- Russia: By using the Services, you consent to the transfer of your personal data from Russia to the United States for processing.
- South Korea: Where required by law, we will retain certain personal data for statutorily-prescribed periods (e.g., 5 years for order/payment records, 3 years for consumer complaint records).
- United Arab Emirates (UAE): This Privacy Policy is governed by the laws of the UAE. Any disputes not settled by mediation will be resolved by arbitration in Dubai under the DIFC-LCIA Arbitration Rules.

15. Right to Lodge a Complaint (EU, UK and Switzerland)

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), Opus commits to resolving complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF, the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. EU, UK, and Swiss individuals with inquiries or complaints should first contact Opus EU/EEA GDPR Representative, whose contact details are available in the Section 16 below.

Opus has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed by Opus please visit <https://bbbprograms.org/programs/all-programs/dpf-consumers> for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See

<https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf>

Below are the contact details for the relevant authorities depending on your location:

European Economic Area (EEA) and European Union (EU)

If you are located within the EEA or the EU, you can contact the relevant supervisory authority accessible [here](#).

United Kingdom (UK)

If you are located in the UK, you can contact the Information Commissioner's Office:

[Information Commissioner's Office \(ICO\)](#)

Switzerland

If you are located in Switzerland, you can contact the Federal Data Protection and Information Commissioner:

[Federal Data Protection and Information Commissioner \(FDPIC\)](#)

16. Contacting Us

EU GDPR representative

For users in the EU/EEA, we have appointed the following Firm to provide the services of a EU/EEA GDPR representative in the Union:

White Bison Solutions GmbH

Email: contact@opus.pro

You can reach out to inquire about all issues related to EU/UK and Swiss privacy and data protection laws.

Contact Information

If you have any questions or comments about this Privacy Policy, the ways in which we collect and use your Personal Data or your choices and rights regarding such collection and use, please do not hesitate to contact us at:

www.opus.pro

contact@opus.pro

[+1 650-281-6039](tel:+16502816039)

580 California St., Suite 1205, SF, CA 94104, United States of America