



Claros Privacy Statement

Effective Date: 06/20/2023

Table of Contents

- Introduction
- Data Protection Officer
- How we collect and use (process) your personal information
- Use of the Claros website
- Cookies and tracking technologies
- Use of the Claros's services
- When and how we share information with third parties
- Transferring personal data to the U.S.
- Data Subject rights
- Security of your information
- Data storage and retention + Open AI Data Privacy
- Questions, concerns, or complaints

Introduction

Claros is a chat-based search company that uses generative AI to assist shoppers on websites.

We understand that you are aware of and care about your own personal privacy interests, and we take that seriously. This Privacy Notice describes Claros's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognize that information privacy is an ongoing responsibility, and so we will from time to time update this Privacy Notice as we undertake new personal data practices or adopt new privacy policies.

Data Protection Officer

Claros is a Delaware corporation with headquarters in Milford, CT in the United States. Claros has appointed their DPO for you to contact if you have any questions or concerns about Claros's personal data policies or practices. If you would like to exercise your privacy rights, please direct your query to Claros's DPO. Claros's DPO's name and contact information are as follows:



Anish Thite

Diva Labs, Inc.

78 Myrtlewood Drive Milford CT 06461

anish@claros.so

How we collect and use (process) your personal information

Claros collects personal information about its website visitors and customers. With a few exceptions, this information is generally limited to:

- Email
- Ip address

We use this information to provide prospects and customers with services.

We do not sell personal information to anyone and only share it with third parties who are facilitating the delivery of our services.

From time to time, Claros receives personal information about individuals from third parties. Typically, information collected from third parties will include further details on your employer or industry. We may also collect your personal data from a third party website (e.g. LinkedIn)

Use of the Claros Website

As is true of most other websites, Claros's website collects certain information automatically and stores it in log files. The information may include internet protocol (IP) addresses, the region or general location where your computer or device is accessing the internet, browser type, operating system and other usage information about the use of Claros's website, including a history of the pages you view. We use this information to help us design our site to better suit our users' needs. We may also use your IP address to help diagnose problems with our server and to administer our website, analyze trends, track visitor movements, and gather broad demographic information that assists us in identifying visitor preferences.

Claros has a legitimate interest in understanding how members, customers and potential customers use its website. This assists Claros with providing more relevant products and services, with communicating value to our sponsors and corporate members, and with providing appropriate staffing to meet member and customer needs.



Cookies and tracking technologies

Claros makes available a comprehensive cookie notice that describes the cookies and tracking technologies used on Claros’s website and provides information on how users can accept or reject them. To view the notice, a popup will show on the Claros website.

Sharing information with third parties

The personal information Claros collects from you is stored in one or more databases hosted by third parties located in the United States. These third parties do not use or have access to your personal information for any purpose other than cloud storage and retrieval. On occasion, Claros engages third parties to send information to you, including information about our products, services, and events.

A list of our third party sub processors can be found here: [Supabase](#), [OpenAI](#), [MongoDB](#), [AWS](#)

We do not otherwise reveal your personal data to non-Claros persons or businesses for their independent use unless: (1) you request or authorize it; (2) it’s in connection with Claros-hosted and Claros co-sponsored conferences as described above; (3) the information is provided to comply with the law (for example, compelled by law enforcement to comply with a search warrant, subpoena, or court order), enforce an agreement we have with you, or to protect our rights, property or safety, or the rights, property or safety of our employees or others; (4) the information is provided to our agents, vendors or service providers who perform functions on our behalf; (5) to address emergencies or acts of God; or (6) to address disputes, claims, or to persons demonstrating legal authority to act on your behalf. We may also gather aggregated data about our services and website visitors and disclose the results of such aggregated (but not personally identifiable) information to our partners, service providers, advertisers, and/or other third parties for marketing or promotional purposes.

The Claros website connects with third party services such as LinkedIn, Twitter and others. If you choose to share information from the Claros website through these services, you should review the privacy policy of that service. If you are a member of a third party service, the aforementioned connections may allow that service to connect your visit to our site to your personal data.



Transferring personal data to the U.S.

Claros has its headquarters in the United States. Information we collect about you will be processed in the United States. By using Claros’s services, you acknowledge that your personal information will be processed in the United States. The United States has not sought nor received a finding of “adequacy” from the European Union under Article 45 of the GDPR. Pursuant to Article 46 of the GDPR, Claros is providing for appropriate safeguards by entering binding, standard data protection clauses, enforceable by data subjects in the EEA and the UK. These clauses have been enhanced based on the guidance of the European Data Protection Board and will be updated when the new draft model clauses are approved.

Depending on the circumstance, Claros also collects and transfers to the U.S. personal data with consent; to perform a contract with you; or to fulfill a compelling legitimate interest of Claros in a manner that does not outweigh your rights and freedoms. Claros endeavors to apply suitable safeguards to protect the privacy and security of your personal data and to use it only consistent with your relationship with Claros and the practices described in this Privacy Statement. Claros also enters into data processing agreements and model clauses with its vendors whenever feasible and appropriate. Since it was founded, Claros has received zero government requests for information.

For more information or if you have any questions, please contact us at anish@claros.so

Data Subject rights

The European Union’s General Data Protection Regulation (GDPR) and other countries’ privacy laws provide certain rights for data subjects. Data Subject rights under GDPR include the following:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right of data portability
- Right to object
- Rights related to automated decision making including profiling

This Privacy Notice is intended to provide you with information about what personal data Claros collects about you and how it is used.



If you wish to confirm that Claros is processing your personal data, or to have access to the personal data Claros may have about you, please contact us.

You may also request information about: the purpose of the processing; the categories of personal data concerned; who else outside Claros might have received the data from Claros; what the source of the information was (if you didn't provide it directly to Claros); and how long it will be stored. You have a right to correct (rectify) the record of your personal data maintained by Claros if it is inaccurate. You may request that Claros erase that data or cease processing it, subject to certain exceptions. You may also request that Claros cease using your data for direct marketing purposes. In many countries, you have a right to lodge a complaint with the appropriate data protection authority if you have concerns about how Claros processes your personal data. When technically feasible, Claros will—at your request—provide your personal data to you.

Reasonable access to your personal data will be provided at no cost. If access cannot be provided within a reasonable time frame, Claros will provide you with a date when the information will be provided. If for some reason access is denied, Claros will provide an explanation as to why access has been denied.

For questions or complaints concerning the processing of your personal data, you can email us at anish@claros.so. Alternatively, if you are located in the European Union, you can also have recourse to the European Data Protection Supervisor or with your nation's data protection authority.

Data storage and retention

Your personal data is stored by the Claros on its servers, and on the servers of the cloud-based database management services the Claros engages, located in the United States. The Claros retains service data for the duration of the customer's business relationship with the Claros and for a period of time thereafter, to analyze the data for Claros's own operations, and for historical and archiving purposes associated with Claros's services. Claros retains prospect data until such time as it no longer has business value and is purged from Claros systems. All personal data that Claros controls may be deleted upon verified request from Data Subjects or their authorized agents. For more information on where and how long your personal data is stored, and for more information on your rights of erasure and portability, please contact us at anish@claros.so.

Open AI API Privacy Policy

Straight from the OpenAI website. Zero data retention requests can be made on a case by case basis for customers.

Zero data retention

We recognize that API customers may handle sensitive information, including customer data, which is subject to data protection regulations. You can request zero data retention (ZDR) for eligible endpoints, and may be asked to meet additional requirements. When ZDR is approved, inputs and outputs will not be stored but may still be run through our safety classifiers.

Some data sent to specific endpoints like `/v1/audio/transcriptions` is not retained. For more information visit our Platform Docs page.

Default usage policies by endpoint

ENDPOINT	DATA USED FOR TRAINING	DEFAULT RETENTION	ELIGIBLE FOR ZERO RETENTION
<code>/v1/completions</code>	No	30 days	Yes 
<code>/v1/chat/completions</code>	No	30 days	Yes 
<code>/v1/edits</code>	No	30 days	Yes 
<code>/v1/images</code> <code>/generations</code>	No	30 days	No
<code>/v1/images/edits</code>	No	30 days	No
<code>/v1/images/variations</code>	No	30 days	No
<code>/v1/embeddings</code>	No	30 days	Yes 
<code>/v1/audio</code> <code>/transcriptions</code>	No	Zero data retention	-
<code>/v1/audio/translations</code>	No	Zero data retention	-
<code>/v1/files</code>	No	Until deleted by customer	No
<code>/v1/fine-tunes</code>	No	Until deleted by customer	No
<code>/v1/moderations</code>	No	Zero data retention	-

For details, see our [API data usage policies](#). To learn more about zero retention, get in touch with our [sales team](#).

Children's data

We do not knowingly attempt to solicit or receive information from children.

Questions, concerns or complaints



If you have questions, concerns, complaints, or would like to exercise your rights, please contact us at:

Claros

Anish Thite

78 Myrtlewood Drive Milford CT 06461

anish@claros.so