

SecureAuth Data Privacy Framework Statement

Effective Date: September 30, 2026

Data Privacy Framework

SecureAuth Corporation complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and 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. SecureAuth Corporation 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 and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. SecureAuth Corporation 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 Statement 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, please visit <https://www.dataprivacyframework.gov/>. To view our certification, please visit <https://www.dataprivacyframework.gov/participant/7834>.

Introduction & What This Statement Covers

We at SecureAuth Corporation ("SecureAuth", "we", "us", "our") care about protecting personal data. This Data Privacy Framework Statement (the "Statement") tells you how we process the personal data we process on behalf of our customers while providing, implementing, and supporting our services.

Our services include our identity and access management solutions, namely:

- the SecureAuth Connect platform, consisting of Consumer Authority, B2B Authority, Workforce Authority (formerly Arculix), and Agent Authority; and
- SecureAuth IdP;

as well as the provision of our consulting services, customer support (via Zendesk and Jira), and other systems that we use to assist our customers (collectively, the "Services").

This Statement also describes how we handle personal data through the services available through the following domains:

- SecureAuth Connect: connect.secureauth.com and its regional and tenant subdomains (us.connect.secureauth.com, eu.connect.secureauth.com and au.connect.secureauth.com);
- Workforce Authority: mfa.acceptto.com, sso.acceptto.com, oidc.acceptto.com and reports.acceptto.com;
- SecureAuth IdP (cloud-hosted): identity.secureauth.com and its tenant subdomains, plus login.secureauth.com. Self-hosted and hybrid deployments are excluded; and
- Support and resources: support.secureauth.com, docs.secureauth.com, downloads.secureauth.com, community.secureauth.com and cloud.secureauth.com.

This Statement does not apply to personal data we collect by other means, such as personal data that we receive directly through our marketing website(s) or the personal data of our employees.

Our customers use our platform to process their own employees', customers', and vendors' personal data. In that case, we act only as a service provider. In general, we only access such personal data if required by law, or if the customer asks us to in connection with customer support or account administration matters in relation to the Services.

Our Role with Respect to Personal Data

SecureAuth acts as an agent, also known as a data processor, for the personal data we process for our customers while providing our Services. This means that the organization that entered into the contract governing use of the Services (the "Customer Agreement") (our "Customer") chooses the type of personal data they give us to process on their behalf. This organization may be your employer or someone else. We usually do not have a direct relationship with the people whose personal data we get from our Customers.

Why We Process Personal Data

We process personal data according to the instructions of our Customers.

How We Obtain Personal Data

We receive personal data:

- From our Customer and its representatives while providing the Services.
- From providers of third-party services that integrate with our Services.
- When the information is submitted to our websites.
- When you participate in a focus group, contest, activity, or event, apply for a job, ask for support, interact with our social media, or otherwise communicate with us.

What Personal Data We Process

We process the following types of personal data:

- Biographical information: name.
- Professional information: company/employer.
- Contact information: email and phone number.
- Account information: username, user ID, and password.
- Usage information: Services metadata, log data, messages, and the date and time the Services are used.
- Device information: device type, unique device identifier, operating system, settings, application ID, crash data, browser type and settings, and host address.
- Location information: location from IP addresses.
- Cookie information and similar tracking information.
- Personal data received from other companies' services.

Our Purposes to Process Personal Data

We process your personal data for the following purposes:

- To provide, update, maintain and protect our Services, websites, and business.
- To follow the law, legal process, or regulation.
- To communicate with you and respond to your requests, comments, and questions.
- To develop and provide search, learning and productivity tools and additional features.
- To send emails and other communications about the Services, including security and account-related communications.
- To administer accounts and keep track of billing and payments.
- To contact you regarding billing, account management, and other administrative matters, such as invoicing and payments tracking.
- To investigate and help prevent security issues and abuse.
- To provide application logs to Customer administrators for troubleshooting and monitoring of the applications.
- To assist our Customers as they request.

How Long We Keep Personal Data

We keep personal data for as long as our Customer instructs us to. We delete the personal data that our Customers give us within six (6) months after our agreement with the Customer ends.

We will not delete this personal data within the six-month period if the law says we have to keep it, the Customer asks us to keep it longer, or the information cannot be traced back to a specific person anymore and it is considered fully anonymized and consequently is no longer considered personal data.

Sharing Personal Data with Third Parties

Purposes for Sharing Personal Data with Other Companies

We share personal data with the following types of service providers for the purposes provided:

- Internet service providers for internet hosting purposes.
- IT service desk service providers for customer service and support ticket management.
- Data analytics service providers for processing, analyzing, and visualizing insights from large datasets.
- Telephone and internet audio and video conferencing service providers for remote communication and screen sharing.
- Cloud desktop service providers for virtual desktop management.
- Customer identity service providers for storage and verification of user identity and engagement.
- Managed service providers for monitoring of IT infrastructure, including networks, servers, applications, and other systems.
- Project management service providers to assist with the achievement of project goals and objectives within scope, time, and budgetary constraints.
- Communications service providers for the delivery of SMS, voice, and email one-time passcodes and notifications.

- Unified communications service providers for email, communications, and collaboration purposes.
- Customer relationship management service providers for customer interaction management and customer support tools.

In the context of an onward transfer of your personal information, SecureAuth remains responsible for the processing of personal information we receive under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF Principles and which we subsequently transfer to a third party acting as an agent on our behalf. As required by law, SecureAuth remains liable under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF Principles if its agent processes such personal information in a manner inconsistent with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF Principles, unless another party is responsible for the event giving rise to the damage.

We also reserve the right to use, transfer, and share aggregated, anonymous data for any legal business purpose. Such data does not include any personal data.

We may disclose your personal data if we sell or transfer all or some of our business interests, assets, or both, or in connection with a corporate restructuring.

How We Share Personal Data with Law Enforcement

We may disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

We disclose your personal data if the law requires it, or if we think it is necessary for official investigations or legal proceedings. These proceedings may be started by government or law enforcement officials, or private parties.

If we must disclose your personal data to governmental or law enforcement officials, we may not be able to ensure that those officials will maintain the privacy and security of your personal data.

Cookies

Cookies are small files that are stored on your device and contain information about your device. We use cookies to show ads, make our websites and Services work better, authenticate you, analyze how our websites and Services are used, remember your settings, and improve our websites and Services.

There are two types of cookies: session cookies and persistent cookies. We use both types of cookies. Session cookies are deleted when you close your browser. Persistent cookies stay on your device even after you close your browser, but they have an expiration date.

Most of the cookies that our Services and websites place on your device are first-party cookies, which means that they are placed directly by us. Other parties, such as Google, may also place their own cookies through our Services. You can read the policies of these third parties to learn more about the way in which they collect and process information about you.

You can change your browser settings to reject all or some cookies if you prefer not to accept them. However, this may limit the features of the Services you can use. You can learn more about cookies and how to manage them by visiting <https://www.aboutcookies.org/>.

You can also set your browser to send a “Do Not Track” signal but note that our Services are not set up to respond to “Do Not Track” signals from browsers. You can learn more about “Do Not Track” signals by visiting <https://allaboutdnt.com/>.

Data Integrity & Security

We have implemented and will maintain reasonably designed technical, administrative, and physical measures to protect personal information from unauthorized access, alteration, destruction, use, or disclosure.

Your Privacy Rights

Upon written request to SecureAuth, SecureAuth will provide individuals from the European Union, the United Kingdom, and Switzerland with reasonable access to personal information that SecureAuth holds about them, and will allow them to correct, amend, or delete such information if it is inaccurate or has been processed in violation of the Data Privacy Framework Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the particular case, or where the rights of other individuals would be violated.

SecureAuth also enables individuals to opt out of the disclosure of their personal information to third parties or its use for purposes materially different from those for which it was originally collected or subsequently consented by the individuals, in compliance with the Data Privacy Framework Principles.

When SecureAuth obtains Personal Data in its role as a Processor for its Customers, SecureAuth's Customers are responsible for providing individuals with access to the Personal Data and the right to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Data Privacy Framework Principles, as appropriate. In such circumstances, individuals should direct their questions to the appropriate SecureAuth Customer. When an individual is unable to contact the appropriate Customer, or does not obtain a response from the Customer, SecureAuth will provide reasonable assistance in forwarding the individual's request to the Customer.

Resolving Disputes

VeraSafe Data Privacy Framework Dispute Resolution Procedure

We have agreed to participate in the dispute resolution process provided by VeraSafe, the VeraSafe Data Privacy Framework Dispute Resolution Procedure ("Dispute Resolution"). This will be used if a complaint or dispute cannot be resolved through our internal procedures. As per the terms of the Dispute Resolution, VeraSafe will provide appropriate recourse free of charge to you. To file a complaint with VeraSafe and participate in the Dispute Resolution, please visit this link:

<https://www.verasafe.com/public-resources/dispute-resolution/submit-dispute/> and submit the required information.

Binding Arbitration

If your dispute or complaint cannot be resolved by us, nor through the dispute resolution program established by VeraSafe, you may have the right to require that we enter into binding arbitration with you pursuant to the Data Privacy Framework's Recourse, Enforcement and Liability Principle and Annex I of the Data Privacy Framework.

U.S. Regulatory Oversight

SecureAuth is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

Changes to this Statement

We may make changes to this Statement from time to time. If we make any material change to this Statement, we will let you know by posting the updated Statement to this web page and updating the “Effective Date” at the top of the Statement.

Contact Us

If you have any questions or concerns about this Statement or how we process your personal data, please reach out to us. You can:

- Email our privacy team at privacy@secureauth.com;
- Call us on 1-866-859-1526; or
- Reach us by postal mail at:
SecureAuth Corporation
49 Discovery, Suite 220
Irvine, CA 92618
U.S.

Please allow up to four weeks for us to reply. We will respond to any complaint regarding our compliance with the Data Privacy Framework Principles within 45 days of receiving it.