Privacy & cookies notice

Last updated: March 31, 2021

We last updated this Privacy Policy on March 31, 2021. You may review a summary of the changes here and the prior version of our Privacy Policy here.

Introduction and Background

Privacy is important to Auth0 and we take care to process personal data in accordance with applicable data protection laws and our contractual obligations. Please take the time to read both this Privacy Policy and the Cookies Notice (together the "Policy") to understand how Auth0 secures personal data, and why and how Auth0 processes, shares and secures personal data, and to learn more about your rights and preferences.

In this Policy, "Auth0," "we," "us" and "our" each means Auth0 Inc. (10800 NE 8th Street, Suite 700, Bellevue, WA 98004, USA) and/or the applicable Auth0 affiliates processing personal data. Auth0 Limited, UK, is registered with the Information Commissioner's Office ("ICO") under registration number ZA840835.

If you have any questions about this Policy, please contact us at privacy@auth0.com.

- What this Policy covers
- Personal data we process and sources of personal data
- Why and how we process personal data
- Personal data sharing and disclosure
- Where we process personal data and international transfers
- Personal data retention and deletion
- Your choices and rights
- Security of your personal data
- Children's privacy
- How to contact Auth0 about privacy
- Changes to this Policy
- Additional information – Europe (including Switzerland and UK)
- Additional information – Residents of California, USA
- Cookies notice

Scope of this Policy

What this Policy covers
This Policy applies where Auth0 processes personal data about human beings in its role as a controller of that personal data. This includes where you:

- Visit our website www.auth0.com or other Auth0 digital properties or branded social media pages (collectively, the “Sites”)
- Are identified as a prospect or potential customer of Auth0
- Receive communications from us (including emails, phone calls or text messages)
- Apply for a job with Auth0 or are referred to us for recruitment reasons
- Visit our offices
- Provide services to Auth0 as a vendor or service provider or contact us for other purposes (e.g. regulatory officials working in their official capacity)
- Are an Auth0 customer or use the Services (as defined below) as a customer or an authorized user (e.g. as an employee of one of our customers or Marketplace partners who provided you access to our Services) where we act as controller of your personal data
- Register for, attend or participate in webinars, sponsored events, trade shows, online surveys, contests or other similar promotional events organized by Auth0
- Participate in the Auth0 Ambassadors program or in the Auth0 Research Program
- Interact with the Auth0 community (community.auth0.com)

What this Policy doesn't cover

This Policy doesn’t apply where we process personal data about our customers’ end users that is input into the Auth0 platform for processing as part of the Services (i.e., where Auth0 acts as a processor).

Auth0 customers (and/or their affiliates) use our services to secure user identities and connect users to their applications via the Auth0 Identity Management Platform (“Auth0 Platform” or “Services”). We process personal data of our customers and their end users in accordance with our customers’ instructions. Our customers control the personal data that is made available to us via the Services. We act as a “processor” (for purposes of the General Data Protection Regulation or “GDPR”) or “service provider” (under the California Consumer Privacy Act or “CCPA”) or similar roles under applicable law on behalf of our customers. Our customers’ privacy policy or agreements with its end users (or the end user’s organization) will apply to such processing, not this Policy. If you are an end user of our customer - please contact that organization for information.

If you are an end user of an Auth0 customer and have questions about personal data used by such customer, or if you want to exercise any of your rights regarding your personal data processed by such customer, we request that you contact the customer directly.

---

Personal data we process and sources of personal data

Information you give us directly:

- **Contact, biographical and payment information** - this includes your contact details, social media handle, financial and credit card information if you are a customer paying directly through our Sites, personal description and photograph, company name and position, login and password details, and
information you share in discussion boards, search queries, feedback forums, or in customer service requests. This may also include audio or video recordings if you participate in a customer interview or testimonial (and where legally permissible).

- **Employment and professional information** - if you apply for a job at Auth0, this includes your CV, resumé or other details about your education and employment history in relation to recruitment activities. In limited circumstances and only where legally permissible, this may include sensitive personal data, such as information about health or disability (e.g. where required for access) or information about ethnicity (e.g. where relevant to local diversity obligations for employment purposes).

**Information we automatically collect from your interactions with us:**

- **Technical information related to your visit to our Sites and/or Services** - this includes your Internet protocol (IP) address (which can provide general information about your location, country, region, or city, but not your precise location), login information, device data such as device/browser type and version, time zone setting, and the operating system and platform you use when visiting our Sites or Services.

- **Information about your use of our Site and Services, and your activities and your interaction with our marketing materials** - this may include the web address of the page you were on prior to coming to our Site and the page you visit after you leave. We may also process information about what you do on our Sites, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, downloads and mouse-overs), methods used to browse away from the page, and data relating to whether you engaged with our marketing materials (e.g. from web beacons). See our [Cookies Notice](#) for more information about your choices in relation to cookies technology.

**Information we obtain from other sources:**

- **Marketing and sales information (including your web browsing activity if cookies are enabled)** - this includes biographical information and job information, contact details, sales orders from third party lead generation resources and marketing list vendors such as ZoomInfo, or from publicly available sources such as LinkedIn. We may receive information about your browsing activities on websites outside of Auth0 collected via partners such as 6Sense. We also receive information from marketing partners and event sponsors where we co-host events and webinars and from digital advertising partners, business partners, advertising networks, analytics providers, and search information providers.

- **Log-in / authentication information and other information related to our provision of the Services** - if you log in to our Site or Services by using credentials from a third party (for example, Google, Microsoft or GitHub), or if you engage a “Third Party Integration” (see the [Auth0 Marketplace Terms of Use](#) for more information) to send information, we will receive information that you (or the Customer on your behalf) have authorized for sharing. Channel partners that offer joint marketing services, or referral or reseller partners of the Services will also pass details to Auth0 in order for us to follow-up with prospective customers and/or to fulfil customer orders.

- **Employment / educational history / background check information** - if you apply for a job at Auth0, our service providers, partners or other agencies, such as recruitment agencies or referees, may provide information in relation to your application for employment with Auth0, including information about immigration status or criminal allegations or offences in relation to compulsory background checks, where legally permissible.
Why and how we process personal data

We use personal data in accordance with applicable legal requirements, including for the following purposes:

- **To administer, monitor the usage of and to improve the Site.** We may use personal data to administer our Site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes and for safety and security including detecting, investigating, and preventing activities on our Site that may violate our terms of use, could be fraudulent, violate copyright, or other rules or that may be otherwise illegal. We may use information to improve our Site, to ensure that content is presented to you in the most effective manner and to allow you to participate in interactive features of our Site when you choose to do so.

- **To provide, monitor the usage of and to improve the Services.** We will use your personal data to provide, monitor the usage of and to improve the Services. This includes concluding contracts; billing and other account administration; provision of user authentication and user authorization; event logging; internal research and product development; ensuring safety and security including detecting, investigating, and preventing activities on our Services that may be fraudulent or may violate copyright, contractual terms, or other rules, or that may otherwise be illegal; monitoring usage of the Service to ensure compliance with Auth0 policies; and conducting data analytics. This also includes provision of customer and technical support for the Services (including the recording of some support services provided via phone or with online conference services such as Zoom).

- **To conduct marketing (including direct marketing) and sales activities.** Where permissible by local law and in accordance with our legitimate interests, we may build and maintain sales & marketing profiles of prospective and actual customers and of individuals representing them in a “customer relationship management” “CRM” database. We may combine information from different sources to better understand their interests and to provide content or information about the Services that are relevant to their business needs. E.g. We may enhance their CRM profile information with information about their activities on the Site or the Services with browsing activities on websites outside of Auth0 collected via partners such as 6Sense in order to target marketing to them and assess how likely they are to purchase Auth0 services. We may also do this to measure the effectiveness of advertising we serve to them and others.

- **Employment purposes.** If you have applied for a job with Auth0, we will use your personal data for employment purposes, including recruitment and selection, to conduct background checks, to conduct onboarding if we decide to hire you, and to meet local legal obligations such as those related to health and safety and, where appropriate, diversity and inclusion.

- **Other business purposes.** We use personal data in accordance with law to administer our global business operations, including physical site operation, for record-keeping and corporate governance purposes, to respond to queries from individuals, and to comply with legal requirements or other such reasonable purposes related to our business operations.
Personal data sharing and disclosure

Auth0 discloses personal data to third parties in accordance with legal and contractual requirements as follows:

To third party service providers who process your personal data on our behalf and in accordance with our instructions and applicable law. These organisations, which will only use your personal data to the extent necessary to perform their support functions, include:

- Operational, security and marketing service providers and other business partners with whom we have entered into agreements in relation to the processing of your personal data.
- Analytics and search engine providers that assist us in the improvement and optimisation of our Site and Services, subject to the Cookies Notice.
- Payment processing providers who provide secure payment processing services. Your payment card details are not shared with us by the provider.

To marketing and analytics partners that work with us in marketing activities, such as creating or organizing gated content, webinars and virtual events. We will only transfer your personal data to our marketing partners in accordance with legal requirements, including with your prior consent where required.

To prospective sellers or buyers in the event that we sell or buy any business or assets, in which case we will disclose your personal data to the prospective seller or buyer of such business or assets, subject to this Policy; or to a third party acquiring all or substantially all of Auth0’s assets, in which case personal data held by Auth0 about its customers will be one of the transferred assets.

To members of the Auth0.com group, which includes Auth0 Inc. and our affiliates, and our subsidiaries who support our processing of personal data under this Policy.

To third parties in order to comply with any legal obligation, or in order to enforce or apply our terms of service, and other agreements with you, or to protect the rights, property, or safety of Auth0, our customers, or others.

Where we process personal data and international transfers

Storage. Auth0 primarily stores your personal data in the United States (“US”) and in the Europe Economic Area (“EEA”). Personal data that is transferred to, or stored at, a destination outside the EEA may not be subject to data protection laws that provide the same level of protection as those in your jurisdiction.

Transfer. Where your personal data originates from the EEA, United Kingdom (“UK”) or from Switzerland and is transferred outside of your jurisdiction, we ensure that your personal data is subject to appropriate safeguards (such as a recognised legal adequacy mechanism or standard contractual clauses with third parties or between Auth0 group companies that process your personal data on our behalf) and that it is treated securely and in accordance with this Policy.

If you are a customer and have questions about transfers of personal data from the EEA, the UK or Switzerland to the US by Auth0, please review our Customer Toolkit for International Data Transfers or our FAQs on EU Data Transfers to the US and Applicable US Laws.
Personal data retention and deletion

- We retain personal data only for as long as is needed to exercise our legal obligations and for appropriate business purposes.
- If you have applied for a job at Auth0, your personal data will usually be deleted 2 years after your application process concludes. You may contact privacy@auth0.com to request that we delete your application and CV information sooner than this.
- We retain personal data during any period in which you have expressed an interest in our Sites or Services, for as long as necessary for us to meet our contractual obligations, and for six years after the end of a contract to identify any issues and resolve any legal proceedings. For clarity, this does not change Auth0's contractual obligations to delete personal data as described in our customer contracts.

At the end of retention periods, Auth0 may retain limited aggregate information for research purposes and to help us further improve our Services. This aggregate information does not include any personal data that relates to you as an individual.

Your choices and rights

- **Opt-out of marketing email communications** You can opt out of direct marketing from Auth0 at any time by checking and updating your contact details within your account, using the "unsubscribe" link at the end of all our marketing emails, or by submitting your email address at the Email Preference Center here. If you are a customer and you opt-out of receiving marketing messages from Auth0, you may continue to receive transactional communications from us regarding our Services.

- **Managing Cookies, Targeted Advertising and Other Tracking/Analytics Technologies** See our Cookies Notice for information about Cookies and Tracking/Analytics Technologies used on our Site and Services and about your options in relation to these technologies including relevant browser-based cookies controls and other opt-out capabilities.

- **Mobile Device Settings** Your mobile device may also have settings that, if enabled, restrict mobile app platforms (such as Apple and Google) from sharing certain information obtained by automated means.

- **“Do-Not-Track”** At this time, we do not respond to web browser “Do-Not-Track” signals. To learn more about browser tracking signals and DNT, visit All About DNT.
Security of personal data

We are committed to maintaining the confidentiality, integrity, and security of your personal data and take precautions to protect such information. It is our policy to use reasonable and appropriate administrative, technical, and physical safeguards designed to protect the personal data we have about you from loss, theft, and unauthorized use, access, modification, or destruction. We periodically review our policies and procedures to confirm that they are appropriate to meet our commitment to our community, our customers, and ourselves.

We also require third-party service providers acting on our behalf or with whom we share your personal data to maintain security measures consistent with applicable regulatory compliance requirements.

Payments made on the Site are made through our payment gateway provider. Payment details you provide will be encrypted using secure sockets layer (SSL) technology before they are submitted to us over the internet. Personal data you supply to our payment gateway provider is not within our control and is subject to the provider's privacy policy and terms and conditions.

Notwithstanding our security safeguards, it is impossible to guarantee absolute security in all situations. If you have any questions about the security of our Site or Services, please contact us at privacy@auth0.com. For your own security, please do not send any confidential or sensitive personal data to us via email or through the contact form on our website.

Children's privacy

The Site is intended for use only by individuals who are at least 16 years of age. By using the Site, you confirm to us that you meet this requirement. If you are under the age of 18, you confirm you have received permission from your parent or guardian before using this Site or sending us personal data.

How to contact Auth0 about privacy

Questions, comments, and requests regarding this Policy are welcomed and should be addressed to:

Privacy Office - Legal Department
Auth0, Inc.
10800 NE 8th Street, Suite 600,
Bellevue, WA 98004, U.S.A.
privacy@auth0.com
We periodically review and update this Policy to describe changes to our data processing practices or to reflect changes in laws and regulations that apply to Auth0. You can check when this Policy was last revised by referring to the “Updated” date at the top of this Policy. We encourage you to review the Policy whenever you interact with us to stay informed about our privacy practices.

If the changes we make to this Policy are significant, we may notify you including through a prominent notice on the Site or the Services, as appropriate. If you do not agree with the privacy practices disclosed in the Policy, we recommend you stop using our Site and Services.

This section applies to individuals located in the EEA, the UK or in Switzerland and outlines additional information about your rights and choices regarding Auth0’s processing of your personal data under the GDPR or equivalent laws in Switzerland and UK.

A. Legal Basis

We collect and process personal data about you only where we have a legal basis for doing so under applicable data protection laws. Our legal bases include processing personal data as follows:

- **With your consent:** Where appropriate or legally required, we collect and use personal data about you subject to your consent (e.g. where legally required for direct marketing activities or to process your application for employment).

- **Performance of contract:** We collect and use personal data about you to contract with you or to perform a contract that you have with us.

- **To protect the legitimate interests of Auth0, you or other parties:** We process personal data for our legitimate interests such as to improve our Site or Services; deliver content; optimize your experience; market our Services; provide appropriate security for the Services; and to protect you, Auth0 and other third parties.

- **Where necessary for compliance with laws:** We may process personal data about you: (1) as required by law, such as to comply with a subpoena or similar legal process; (2) when we believe in good faith that disclosure is necessary to protect our rights or property, to protect your health and safety or the health and safety of others; (3) to investigate fraud or respond to a government request; or (4) if we are involved in a merger, acquisition, or sale of all or a portion of our assets.

B. Data Subject Rights

You have certain rights related to the personal data we hold about you in our capacity as “controller.” Some of these rights may be subject to limitations and qualifications including (1) where fulfilling your request would adversely affect other individuals, company trade secrets or intellectual property; (2) where there are overriding public interest reasons; or (3) where we are required by law to retain your personal data.
• **Right of Access:** You have the right to access personal data held by us.

• **Right to Rectification:** You have the right to rectify personal data that is inaccurate or incomplete.

• **Right to Data Portability:** You have the right to request a copy of certain personal data we hold about you in a structured, machine readable format, and to ask us to share this information with another entity.

• **Right to Erasure:** You have the right to have personal data deleted where: (1) you believe that it is no longer necessary for us to hold your personal data; (2) we are processing your personal data based on legitimate interests and you object to such processing and we cannot demonstrate an overriding legitimate ground for the processing; (3) you have provided your personal data to us with your consent and you wish to withdraw your consent and there is no other ground under which we can process your personal data; or (4) where you believe the personal data we hold about you is being unlawfully processed by us.

• **Right to Restrict Processing:** You have the right to ask us to restrict (stop any active) processing of your personal data where: (1) you believe the personal data we hold about you is inaccurate and while we verify accuracy; (2) we want to erase your personal data as the processing is unlawful, but you want us to continue to store it; (3) we no longer need your personal data for our processing, but you require us to retain the data for the establishment, exercise, or defense of legal claims; or (4) you have objected to us processing your personal data based on our legitimate interests and we are considering your objection.

• **Right to Object:** You can object to our processing of your personal data based on our legitimate interests. We will no longer process your personal data unless we can demonstrate an overriding legitimate purpose.

• **Objection to Direct Marketing, Automated Decision Making, and Profiling:** You have the right to object to our processing of personal data for direct marketing communications, and profiling related to direct marketing. We will stop processing the personal data for that purpose.

• **Automated Profiling:** In the event that we conduct automated decision making that has a legal or other significant impact we will tell you about this and you have the right to challenge such decisions and request that it is reviewed by a human.

• **Withdrawal of Consent:** Where the processing of your personal data by us is based on consent, you have the right to withdraw that consent without detriment at any time by emailing privacy@auth0.com or other means provided.

**C. Exercising your Rights**

If you would like to exercise the rights set forth above, please contact us at privacy@auth0.com. Before we respond to requests for personal data, we will require that you verify your identity or the identity of any data subject for whom you are requesting personal data. Our verification methods may include requesting that you log into your account, confirm your contact information or email address, and/or provide documents for identity verification depending on the nature of your relationship with us.

We will fulfil your request within one month of receipt unless an exception applies. If you have concerns unresolved by Auth0, you may also address any grievance directly with the relevant Supervisory Authority or the ICO for UK-based individuals.
We will fulfill your request within one month of receipt unless an exception applies. If you have concerns unresolved by Auth0, you may also address any grievance directly with the relevant Supervisory Authority or the ICO for UK-based individuals.

D. Contact Details for Auth0's Data Protection Officer and EU Representative

Auth0, Inc. (10800 NE 8th Street, Suite 600, Bellevue, WA 98004, USA) is the controller for personal data collected in connection with the use of the Site and Services in the EEA, the UK and Switzerland. Our Data Protection Officer can be contacted at privacy@auth0.com.

For EU personal data protection, Auth0 has nominated a GDPR Representative Lionheart Squared who may be contacted at:

Lionheart Squared (Europe) Ltd.,
2 Pembroke House, Upper Pembroke St 28 –32,
Dublin, D02 EK84, Ireland
auth0@lionheartsquared.eu

E. About the Privacy Shield

We are committed to complying with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data transferred from the EEA, UK and Switzerland to the United States pursuant to Privacy Shield. We have certified that we adhere to the Privacy Shield Principles with respect to such personal data. If there is any conflict between this Policy and the data subject rights under the Privacy Shield principles, the Privacy Shield principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit here.

We are aware that, on July 16, 2020, the European Court of Justice invalidated the EU-US Privacy Shield as a means of ensuring adequate protection for personal data transferred to the US. We are also aware that the Swiss Data Protection Authority and Information Commissioner invalidated the Swiss-US Privacy Shield in September 2020. In reflection of these rulings, where we transfer personal data originating in the EEA, UK or in Switzerland to the US, transfers are made under the Standard Contractual Clauses approved by the European Commission.

By continuing our commitment to the EU-US Privacy Shield and the Swiss-US Privacy Shield frameworks, we remain subject to the investigatory and enforcement authority of the United States Federal Trade Commission (FTC). Furthermore, pursuant to the Privacy Shield principles, we still acknowledge the right of individuals located in the EEA, UK or in Switzerland to access, inspect, update or correct their personal data. Individuals located in the EEA, UK or in Switzerland may exercise their rights by emailing Auth0 at: privacy@auth0.com.

Under the Privacy Shield, we may be liable for the onward transfer of personal data to third parties as described under the Personal data sharing and disclosure section. If we receive personal data subject to our certification under the Privacy Shield and then transfer it to a third-party service provider acting as an agent on our behalf, we have certain liability under the Privacy Shield if both (i) the agent processes the personal data in a manner inconsistent with the Privacy Shield and (ii) we are responsible for the event giving rise to the damage. We may be required to release personal data in response to lawful requests by public authorities including to meet national security and law enforcement requirements.

In compliance with the Privacy Shield principles, we commit to resolving complaints about your privacy and our collection or use of your personal data transferred to the US pursuant to Privacy Shield. Individuals located in the EEA, UK or in Switzerland with Privacy Shield inquiries or complaints may email Auth0 at compliance@auth0.com or write to us at:
We have further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit here for more information and to file a complaint. This service is provided free of charge to you. If your Privacy Shield 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 Privacy Shield Annex 1 here.

Additional information – Residents of California, USA

This section applies to California residents and outlines your rights and choices with respect to Auth0's processing of your personal data under the CCPA.

For business purposes in the last twelve months, we may have collected, used, and shared personal data about you as described in this Policy. To learn more about the personal data we collect, including the specific pieces of personal data collected, sources of collection, our purposes for collection, and the categories of service providers with whom we share personal data, please see the Personal data we process and sources of personal data, Why and how we process personal data and Personal data sharing and disclosure sections of this Policy.

We do not sell personal data for business or commercial purposes.

A. Consumer Rights

The CCPA grants California consumers certain rights in connection with the personal data collected by businesses, as described below:

- **Right to Know**: You have the right to know the categories and specific pieces of personal data we have collected about you in the previous 12 months.
- **Right to Deletion**: You have the right to request that we delete any personal data we have collected about you.
- **Right to Request Information**: You have the right to request information about our collection, sale, and disclosure of your personal data from the previous 12 months.
- **Right to Opt-out of the Sale of Personal Data**: You have the right to opt-out of the sale of personal data we have collected about you. As of the date of this Policy, Auth0 does not sell the personal data we have collected about you.
- **Right to Non-Discrimination**: You have the right to not receive discriminatory treatment for exercising any of your CCPA rights. We will not treat you differently for exercising any of the rights described above.

B. Exercising Your Rights
To exercise any of the CCPA rights above, please contact us by emailing privacy@auth0.com. We will fulfill your request within 45 days of receiving your request. Some of these rights may be subject to limitations and qualifications, such as where fulfilling the request would conflict with federal, state or local law, regulatory inquiries, subpoenas or Auth0's ability to defend against legal claims.

We will verify your request using your email address. If you've created an account with us, we will also verify your request using the information associated with your account, including billing information. Government identification may be required. We cannot respond to your request if we cannot verify your identity and/or authority to make the request on behalf of another and confirm the personal data relates to you. Making a verifiable consumer request does not require you to create an account with us.

If you wish to use an authorized agent to submit a request to opt-out on your behalf, you must provide the authorized agent written permission signed by you, the consumer. We may deny a request from an authorized agent if the agent cannot provide to Auth0 your signed permission demonstrating that they have been authorized to act on your behalf.

Cookies notice

Cookies and other technologies use by Auth0

We use cookies and/or other similar technologies such as pixel tags or web beacons on our Site and Services to collect and store certain information. We use different types of cookies as listed below.

Cookies and similar technologies enable you to be remembered when using that computer or device to interact with the Site and Services and can be used to manage a range of features and content as well as storing searches and presenting personalised content. Our Site and Services use cookies and similar technologies to distinguish you from other users of our Site and Services. Specifically we use cookies to:

- Administer and secure the Site and our Services
- Provide certain functionality within our Services
- Enhance user experience
- Analyze the Site and Services usage and trends
- Analyze browsing behavior outside of Site
- Track users' movements around the Site and the Services
- Gather demographic data about users
- Deliver advertisements such as online and offline targeted advertising on the Site and inform other marketing communication
- Perform analytics and marketing integration

A number of cookies and similar technologies we use last only for the duration of your web or app session and expire when you close your browser ("session cookies"). Others are used to remember you when you return to the site and will last for longer ("persistent cookies"). A further distinction is between first party cookies which are served directly by us to your Device and third-party cookies which are served by a third party on our behalf.

How to manage cookies
Most web browsers automatically accept cookies and similar technologies, but if you prefer, you can change your browser to prevent this. However, you may not be able to take full advantage of our Site and Services if you do so.

See here for information about managing cookies, including opting out, on different browsers:

- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox
- Safari

Most advertising networks also offer you the option to opt out of targeted advertising. For more info, visit YourAdChoices or Your Online Choices.

To opt-out of Google Analytics, visit here. If you have accounts with third-party providers, such as Facebook or LinkedIn you may be able to control your ad preferences through your account. To learn more about preference-based advertising, change your preferences, or to opt-out, visit NAI Opt-out or DAA Opt-out.

**Cookies that have been set in the past**

If you disable one or more cookies we may continue to use information collected from cookies before they were disabled. However, disabling cookies will prevent further collection of any information. This does not impact any of your rights as detailed elsewhere in the Policy.

**Types of Cookies used**

**Strictly Necessary Cookies**

These cookies are necessary for the Sites and Services to function. Cookies categorized as Strictly Necessary cannot be turned off. These cookies are essential in order to enable visitors to move around the Site and Services and use their features, such as accessing secure areas of the Site. Without these cookies, some key services cannot be provided.

**Performance Cookies**

These cookies collect information about how visitors use the Site or Services, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don’t collect information that on its own individually identifies a Site visitor or Service user.

**Functional Cookies**

These cookies enable the Site to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to the pages of our Sites.

If you do not allow these cookies then some or all of these services may not function properly.

For example, Auth0 uses Google Analytics to track and optimize our Site's and Services' performance and marketing activities. Google Analytics first-party cookies collect information about how users use our Sites. This information is used to compile reports and to help us improve our Site. The reports disclose website trends without identifying individual visitors. For more information about how Google uses information from websites and online services that use the Google Analytics services, please visit here.
For more information on how to opt out of Google Analytics tracking across all websites you use, please visit [here](#).

**Targeting Cookies**

These cookies may be set through our Site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites.

They do not store directly personal data, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

See [here](#) for a list of Cookies used on Auth0 Site and Services.